
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**RECOMMENDATIONS AND PRIVACY REQUIREMENTS FOR A BRING-YOUR-OWN-DEVICE USER POLICY AND AGREEMENT**

by

Chad R. Wedel
Andrew T. Michalowicz

March 2015

Thesis Advisor: Paul C. Clark
Second Reader: Grant M. Wagner

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

# REPORT DOCUMENTATION PAGE

*Form Approved OMB No. 0704-0188*



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | March 2015 | Master's Thesis |

**4. TITLE AND SUBTITLE**
RECOMMENDATIONS AND PRIVACY REQUIREMENTS FOR A BRING-YOUR-OWN-DEVICE USER POLICY AND AGREEMENT

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Chad R. Wedel and Andrew T. Michalowicz

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
N/A

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number N/A.

**12a. DISTRIBUTION/AVAILABILITY STATEMENT**
Approved for public release; distribution is unlimited

**12b. DISTRIBUTION CODE**
A

**13. ABSTRACT (maximum 200 words)**

The purpose of a bring-your-own-device (BYOD) program is to increase productivity as it allows individuals to access and manipulate data from non-traditional workplaces to support mission requirements. The United States Marine Corps (USMC) has started a pilot BYOD program, but a user policy for the USMC BYOD program has not yet been identified, despite the driving force that policy has on final implementation and potential acceptance. Therefore, this thesis answers the question, is it possible to develop a BYOD user policy for the USMC that minimizes risk for all parties while allowing for the intended flexibility?

Three case studies were conducted on organizations that have implemented BYOD programs, comparing user policies and best practices to mitigate risks and address user privacy concerns. The case studies were also compared with governing Department of Defense instructions and National Institute of Standards and Technology guidance to identify a baseline of applicable security controls to formulate a viable user policy and agreement to support USMC security requirements.

This thesis found that a clearly articulated user agreement tailored to the USMC's technological solution can be written to support the successful implementation of its BYOD program to ensure the benefits outweigh the potential risks.

**14. SUBJECT TERMS**
bring-your-own-device; BYOD; mobile device; personally owned mobile device; privacy; user policy; user agreement; United States Marine Corps; USMC; BYOD pilot program; BYOD case study; BYOD implementation; BYOD considerations; BYOD recommendations; BYOD technology; security controls; policy development; acceptable use policy; AUP; rules of behavior; RoB

**15. NUMBER OF PAGES**
159

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# RECOMMENDATIONS AND PRIVACY REQUIREMENTS FOR A BRING-YOUR-OWN-DEVICE USER POLICY AND AGREEMENT

Chad R. Wedel
Lieutenant Commander, United States Navy
B.S., Kansas State University, 1999

Andrew T. Michalowicz
Lieutenant, United States Navy
B.S., United States Naval Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS**

from the

**NAVAL POSTGRADUATE SCHOOL**
**March 2015**

Authors: Chad R. Wedel

Andrew T. Michalowicz

Approved by: Paul C. Clark
Thesis Advisor

Grant M. Wagner
Second Reader

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

The purpose of a bring-your-own-device (BYOD) program is to increase productivity as it allows individuals to access and manipulate data from non-traditional workplaces to support mission requirements. The United States Marine Corps (USMC) has started a pilot BYOD program, but a user policy for the USMC BYOD program has not yet been identified, despite the driving force that policy has on final implementation and potential acceptance. Therefore, this thesis answers the question, is it possible to develop a BYOD user policy for the USMC that minimizes risk for all parties while allowing for the intended flexibility?

Three case studies were conducted on organizations that have implemented BYOD programs, comparing user policies and best practices to mitigate risks and address user privacy concerns. The case studies were also compared with governing Department of Defense instructions and National Institute of Standards and Technology guidance to identify a baseline of applicable security controls to formulate a viable user policy and agreement to support USMC security requirements.

This thesis found that a clearly articulated user agreement tailored to the USMC's technological solution can be written to support the successful implementation of its BYOD program to ensure the benefits outweigh the potential risks.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AD | Active Directory |
| AES | advanced encryption standard |
| AP | access point |
| APL | approved products list |
| ATO | authority to operate |
| | |
| BYOD | bring your own device |
| | |
| C4 | command, control, communications and computers |
| CFAA | Computer Fraud and Abuse Act |
| CIA | confidentiality, integrity and availability |
| CIO | chief information officer |
| CMD | commercial mobile devices |
| CND | Computer Network Defense |
| CPG | consumer packaged goods |
| CSA | cognizant security authority |
| CUI | controlled unclassified information |
| | |
| DAA | designated approving authority |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| DON | Department of the Navy |
| | |
| EEO | equal employment opportunity |
| EEOC | Equal Employment Opportunity Commission |
| ESI | electronically stored information |
| | |
| FCRP | Federal Rules of Civil Procedure |
| FIE | foreign intelligence entity |
| FIPS | Federal Information Processing Standards |
| FLSA | Fair Labor Standards Act |
| FY | fiscal year |

| | |
|---|---|
| GAO | Government Accountability Office |
| GFE | government furnished equipment |
| GPS | Global Positioning System |
| IA | information assurance |
| IATF | Information Assurance Technical Framework |
| ICA | independent computing architecture |
| ID | Identification |
| IG | Inspector General |
| ISP | Internet service providers |
| IT | information technology |
| JPAS | Joint Personnel Adjudication System |
| MAM | mobile application management |
| MCEN | Marine Corps enterprise networks |
| MCNOSC | Marine Corps Network Operations and Security Center |
| MDM | mobile device management |
| NAC | network access control |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| OEM | original equipment manufacturers |
| OPSEC | operational security |
| OS | operating system |
| PC | personal computer |
| PII | personally identifiable information |
| PIN | personal identification number |
| PKI | public key infrastructure |
| RAM | random access memory |
| RDP | remote desktop protocol |
| RoB | rules of behavior |

| | |
|---|---|
| SAAR | system access authorization request |
| SCA | Stored Communications Act |
| SDO | staff duty officer |
| SE | security enhancement |
| SES | Senior Executive Service |
| SF50 | Standard Form 50 |
| SSL | secure socket layer |
| STIG | Security Technical Implementation Guide |
| | |
| TH2 | trusted handheld |
| TPM | trusted platform module |
| TTB | Tobacco Tax and Trade Bureau |
| | |
| USAO | United States Attorney's Office |
| USMC | United States Marine Corps |
| | |
| VDI | virtual desktop infrastructure |
| VMI | Virtual Mobile Infrastructure |
| VPN | virtual private network |

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

This research could not have been accomplished without the assistance of numerous people, and the authors would specifically like to thank and recognize the following individuals:

- We would first and foremost like to thank our Father in Heaven for carrying us through this process.

The authors would also like to thank:

- Paul C. Clark, our primary advisor. Thank you for the enduring patience, time, mentorship, and consistent guidance. We are forever grateful.
- Grant M. Wagner, our 2nd reader. Thank you for the brilliant insights and suggestions.
- Robert L. Anderson, Headquarters U.S. Marine Corps. Thank you for your leadership, time, and constant willingness to support.
- Robert Hughes, Kimberly Hancher, and the Consumer Packaged Goods Firm representative. Thank you for generously devoting time and valuable insight to support our research efforts.
- J.D. Fulp. Thank you for providing methodology and resource recommendations vital to addressing our research questions.
- Master Sergeant William Hess. Thank you for giving us the idea to pursue this research topic.
- Our families. To our wives, Jill and Stacey, and children, Cade and Landree, thank you for your patience and support while we spent countless hours away from home, studying and attending classes. Your consistent understanding, sacrifice, and perseverance during this assignment were a source of inspiration.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

One consequence of cheap, small, and powerful mobile devices constantly connected to the Internet is that many individuals consider their mobile devices as necessary personal appliances, much like a wristwatch in prior decades. Such people refer to their personal devices regularly throughout the day to check email, text messages, social media updates, sporting event scores, etc. This behavior has led to a movement called bring-your-own-device (BYOD), because these users would prefer to use their personal devices as their work device that creates what is known as a "dual use" capability. This movement has advantages and risks for the employee, as well as the employer.

The BYOD trend has taken root in numerous areas of both the commercial sector, as well as organizations within the federal government. BYOD provides organizations an alternative method for connecting the workforce and can offer the unique capability of using a mobile device based on personal preferences for both private and corporate activities. The flexibility that BYOD provides can redefine the concept of a workspace, while also reducing the overhead associated with information technology (IT) and wireless expenditures. This reduction in organizational overhead is realized through the sharing of costs between the employee and the enterprise. Users will pay the costs for voice and data plans while the enterprise funds the management of the devices and the capabilities for accessing work data on their personally-owned devices.[1] Despite these advantages with BYOD, both sides need to understand the challenges and risks prior to implementation. Vital components of any BYOD program are the development and implementation of policy to ensure that both the device and data are secure, while also promoting user personal privacy. The Department of Defense (DOD) has recognized the compelling benefits of BYOD, and consequently, identified it as a long-term objective

[1] Nicole Blake Johnson, "Marine Corps Strategy Could Enable BYOD," *Federal Times*, March 7, 2014, http://www.federaltimes.com/article/20140307/MOB/303070009/Marine-Corps-strategy-could-enable-BYOD.

within the DOD Commercial Mobile Device Implementation Plan.[2] However, the lack of existing DOD policies is one of several obstacles preventing the adoption of BYOD.[3] For its part, the United States Marine Corps (USMC) has developed a BYOD pilot program in line with the Marine Corps Commercial Mobile Device Strategy and the DOD Commercial Mobile Device Implementation Plan.[4,]

## A. BACKGROUND

Since 2012, Headquarters U.S. Marine Corps, Command, Control, Communications, and Computers Department (C4), Cybersecurity Division has been engaged in the planning and development of a BYOD pilot program focused on mobile devices being incorporated into unclassified networks. Implementation of a BYOD program aims to foster enhanced productivity, as it allows members to access and manipulate data from non-traditional work places to support mission requirements.[5] Moreover, BYOD has the potential to create substantial savings when compared to current USMC mobile phone expenses, and establishes avenues for saving in other areas.[6] The ability to leverage hardware, for which the employee has already paid, establishes a cost-sharing model and eliminates some of the redundancy associated with providing government furnished devices and data plans to employees who prefer to use a personally-owned mobile device.

The U.S. Navy and USMC currently spend a significant amount annually on the maintenance, procurement, and data plans associated with unclassified government

---

[2] Department of Defense, *DOD Commercial Mobile Device Implementation Plan*, Department of Defense Memorandum (Washington, DC: Department of Defense, 2013), 16, http://www.defense.gov/news/dodcMdimplementationplan.pdf.

[3] Ibid.

[4] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy* (Washington, DC: Headquarters, U.S. Marine Corps, 2013), 3, http://www.hqmc.marines mil/Portals/156/Newsfeeds/SV%20Documents/20130411_Marine_Corps_Commercial_mobile_device_strategy_Final.pdf; Department of Defense, *DOD Commercial Mobile Device Implementation Plan*, 16.

[5] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 3.

[6] Rita Boland, "Pocket to Payload, Personal Technologies Serve the Marine Corps Environment," *Signal Online*, April 1, 2014, http://www.afcea.org/content/?q=node/12513.

furnished mobile devices. In fiscal year (FY) 2013, the Department of the Navy (DON) spent $60.2 million on government furnished mobile devices and associated data plans with the USMC portion being $14.8 million.[7] For the first 10 months of FY14, the total DON expenditures are similar at $45.2 million spent on mobile devices with the USMC's costs at $11.1 million.[8] BYOD can be leveraged within the DON to capitalize on the fact that most individuals already own portable and mobile devices of their preference that can also be used for work related activities.

According to a study conducted by Pew Research, 58 percent of Americans own a smartphone as of January 2014.[9] Within this overall percentage, 83 percent of the American population within the 18–29 age range owns a smartphone and 74 percent of 30–49 year olds own a smartphone.[10] Another study conducted by Edison Research found similar results.[11] A related study conducted by the Pew Research Center identified that 85 percent of smartphone owners within the 18–29 age range are the most likely to utilize their smartphones to go online, while the 30–49 age range is not far behind at 73 percent.[12] Over 50 percent of these individuals also utilize email services via their smartphones.[13] These statistics translate to an enormous age demographic within the USMC and Navy ranks, as shown in Table 1, who utilize and understand the flexibility that mobile devices provide. According to 2013 demographics, 82.9 percent of active

[7] Leontine P. Thompson (Strategic Sourcing Manager, Naval Supply Systems Command (NAVSUP) Fleet Logistics Center (FLC), San Diego, CA) e-mail message to the author, September 23, 2014.

[8] Ibid.

[9] "Cell Phone and Smartphone Ownership Demographics," accessed December 22, 2014, http://www.pewinternet.org/data-trend/mobile/cell-phone-and-smartphone-ownership-demographics/.

[10] Ibid.

[11] Tom Webster, "2014 Smartphone Ownership Demographics," *Edison Research*, April 25, 2014, http://www.edisonresearch.com/2014-smartphone-ownership-demographics/.

[12] Maeve Duggan and Aaron Smith, "Cell Internet Use 2013," *Pew Research Internet Project*, September 16, 2013, http://www.pewinternet.org/2013/09/16/main-findings-2/.

[13] Ibid.

duty Marines are between the ages of 18 to 30 years old.[14] Active duty U.S. Navy service members within the same age range comprise 64.6 percent of the total force.[15]

Table 1. U.S. Military Age Demographics[16]

| Age Distribution of Active Duty Force | | | | | | |
|---|---|---|---|---|---|---|
| **Service** | **18–21** | **22–30** | **31–40** | **41–50** | **51–59** | **Average** |
| **Marines** | 36.9% | 46% | 14.0% | 3.1% | 0.2% | 25 |
| **Navy** | 18.6% | 46% | 26.3% | 8.3% | 0.8% | 29 |
| **Army** | 18.3% | 48% | 25.6% | 7.9% | 0.7% | 29 |
| **Air Force** | 14.4% | 46% | 28.3% | 10.0% | 0.6% | 30 |
| **Coast Guard** | 12.2% | 48% | 27.0% | 12.0% | 1.0% | 30 |

Many companies have adapted policies and practices to incorporate personally-owned smartphones, tablets and even laptops into their network infrastructure.[17] This practice creates a dual-use device for employees that can be used for both personal and business purposes. The private and public sector entities that have adopted BYOD solutions report that allowing employees to use their personal mobile devices to access company resources often results in increased employee productivity and job satisfaction.[18] Although the USMC has made significant progress regarding technological solutions, significant questions remain regarding BYOD user policy and privacy considerations.

---

[14] Defense Manpower Research, "Demographics of Active Duty U.S. Military," Statistic Brain, November 23, 2013, http://www.statisticbrain.com/demographics-of-active-duty-u-s-military/.

[15] Ibid.

[16] Ibid.

[17] Teena Hammond, "Unavoidable: 62 Percent of Companies to Allow BYOD by Year's End," *ZDNet*, February 4, 2013, http://www.zdnet.com/article/unavoidable-62-percent-of-companies-to-allow-byod-by-years-end/.

[18] "Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," footnote 2, August 23, 2012, http://www.whitehouse.gov/digitalgov/bring-your-own-device.

## B. BYOD RISKS

The adoption of a BYOD program does not come without risks for the employer. These risks fall into two main categories. The first relates to the control of organizational data, namely personally identifiable information (PII) and other sensitive but unclassified data.[19] The second pertains to user behavior while utilizing a personally-owned device to access organizational resources.[20]

A BYOD program also introduces concerns for the employee. These concerns stem from the employee expectation of privacy while using a personally-owned device. Employees must be assured that personal activities conducted and personal data resident on their device will remain confidential and not accessible or subject to organizational monitoring. Conversely, the organization must have the ability to monitor employee activity and control organizational information while the device is utilized for conducting work for the organization. For example, some employees may think that acceptable use policies should not be as stringent since they are using their personally-owned device. This issue opens the door for a possible decrease in worker productivity while also increasing security concerns. Security risks associated with acceptable user behavior—while ensuring user privacy—are key factors for considering whether BYOD can be a worthwhile and successful endeavor for both the employee and the organization.

Prior to signing up for participation in a BYOD program, employees will want assurance that they maintain the freedom to use their personally-owned devices as they please and are not subsequently constrained by the policies set forth by the employer. Additional issues pertinent to the USMC that should be considered are: liability if the device is used by an employee to commit a crime, using a device to conduct work during government furloughs, the transfer or separation of employees, and lost or stolen devices to name a few. These concerns from both sides can be addressed through policy, but despite the driving force that policy has on final implementation and potential

[19] Garry G. Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions,* The Littler Report (New York, NY: Littler Mendelson, P.C., 2012), 8.

[20] Ibid.

acceptance, a BYOD user policy for the USMC BYOD program has not yet been identified.

## C. PROBLEM STATEMENT

Because a BYOD user policy and associated user agreement is crucial to a secure and user friendly BYOD program within USMC networks, this thesis answers the question, is it possible to develop a BYOD user agreement for the USMC that minimizes risk for all parties while also allowing for the intended flexibility? To answer this primary question, it became apparent that the following secondary questions had to be answered.

- What technological solutions and controls are employed by existing BYOD programs, and how do they affect the user policy and agreement?
- What user policy and agreement practices can be leveraged from existing BYOD programs to mitigate USMC security concerns, such as the control and protection of organizational data, secure remote authentication, and compromised personally-owned mobile devices?
- Aside from the security controls required to formulate a viable user agreement, should additional considerations be addressed prior to implementing a BYOD program within the USMC?
- How is "user privacy" defined as it relates to personally-owned mobile devices utilized within a BYOD program?
- What organizational policies are necessary to address and support user privacy on personally-owned devices operating within USMC networks?

User agreements as determined by acceptable use policies and user privacy considerations associated with a BYOD program were the focus of this research effort. User agreements are commonly referred to as rules of behavior (RoB); however, for the purpose of this research, "user agreement" will be the norm.

From the perspective of the USMC, the primary challenges associated with a BYOD program are the following.

- Ensuring the integrity of the mobile operating system (OS).
- Secure remote authentication from the mobile device to organizational servers.

- The protection and control of organizational networks, as well as the data stored on a personally-owned device.[21]

To effectively meet these challenges, the device owner must take an active and defined roll, which must be clearly spelled out in a user agreement.

On the other hand, because employee satisfaction is necessary to make BYOD attractive to the end users, the issue of privacy must also be addressed, such that the limitations on the USMC are also clearly spelled out in a user agreement, so that the users have an accurate understanding of their expectation of privacy.

## D. MOBILE DEVICE DEFINITION

Governing documents provide various mobile device characteristics. To provide a clear definition, it is, therefore, important to identify how a mobile device is characterized within these sources and then how a mobile device was defined for the purpose of this research.

As noted in National Institute of Standards and Technology (NIST) Special Publication 800-124 Revision 1 (SP-800-124), mobile device features are constantly changing.[22] As such, it is challenging to define the term "mobile device." Furthermore, as mobile device features change, so do threats and the necessary security controls to mitigate them.[23] The following hardware and software characteristics collectively define the mobile device baseline as delineated in the SP-800-124.

- A small form factor
- At least one wireless network interface for network access and data communications. This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
- Local built-in (non-removable) data storage

---

[21] Robert Anderson (Chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), in discussion with the author, September 23, 2014.

[22] Murugiah Souppaya, Karen Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication (SP) 800-124 Revision 1 (Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, 2013), 2–3, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[23] Ibid.

- An OS that is not a full-fledged desktop or laptop OS
- Applications available through multiple methods (i.e., provided with the mobile device, accessed through web browser, or acquired and installed from third parties)[24]

NIST SP-800-124 highlights additional mobile device features that should be considered with regard to security risks, such as the following.

- Digital cameras and the ability to capture video
- Microphone and speakers
- Network services:
  - Wireless personal area network interfaces, such as Bluetooth
  - Wireless network interfaces for voice communications, such as cellular
  - Global Positioning System (GPS), which enables location services
- Storage: Support for removable media and support for using the device itself as removable storage for another computing device
- Built-in features for synchronizing local data with a different location (i.e., desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.)[25]

The U.S. Government Accountability Office (GAO) defines a smartphone as:

> A smartphone has more capabilities than a cellphone. Consumers can use smartphones to run a wide variety of general and special-purpose software applications. Smartphones typically have a larger graphical display with greater resolution than cellphones and have either a keyboard or touch-sensitive screen for alphanumeric input. Smartphones also offer expansion capabilities and other built-in wireless communications (such as WiFi and Bluetooth services).[26]

The GAO describes a tablet personal computer as a "portable personal computer with a touch-sensitive screen. The tablet form is typically smaller than a notebook computer but larger than a smartphone."[27]

---

[24] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 2–3.

[25] Ibid.

[26] U.S. Government Accountability Office, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged: Report to Congressional Committees* (GAO-12-757) (Washington, DC: U.S. Government Accountability Office, 2012), 3, http://www.gao.gov/assets/650/648519.pdf.

[27] Ibid.

As this research primarily supports USMC BYOD efforts, the following mobile device definition was used, as stated in the DOD Mobile Device Strategy and the U.S. Marine Corps Mobility Strategy.

> A mobile device is a handheld computing device with a display screen that allows for user input (e.g., touch screen, keyboard). When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information given device limitations (i.e., screen size, computing power). Mobile devices provide the conveniences of conventional desktops or laptop computers in a more portable package. Examples of popular mobile devices include smart phones and tablets.[28]

Laptop computers are not included in this definition.

## E. METHODOLOGY AND SCOPE OF WORK

To identify a baseline user agreement solution specific to the USMC's BYOD program, as well as practices employed to safeguard user privacy, three organizations that had implemented a BYOD program were studied: two BYOD implementations from non-DOD U.S. government organizations, and one commercial sector BYOD implementation. These three implementations, comprised of both private and public sector organizations, were compared and contrasted to obtain a starting point to develop a user agreement for the USMC. The security controls identified within these case studies were also compared with governing DOD instructions and NIST guidance to further refine a baseline of applicable security controls necessary to formulate a viable user agreement. The proposed user agreement was developed to address the USMC's primary security requirements and was tailored to the USMC's technological solutions.

The researchers are not qualified to interpret law or provide legal opinions; therefore, complex legal issues associated with the implementation of a BYOD program were not the focus of this research. However, certain legal aspects related to employee privacy, user agreements and restrictions, and control of organizational data are discussed. The final product is a proposed BYOD user agreement that clearly identifies

[28] Department of Defense, *DOD Mobile Device Strategy*, Department of Defense Memorandum, (Washington, DC: DOD, 2012), i, http://www.defense.gov/news/dodmobilitystrategy.pdf; Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 4.

participant responsibilities and addresses potential privacy concerns. Programs to incentivize BYOD participation and a cost-benefit analysis were not the focus of this research and are not addressed in depth. In line with the DOD definition of a mobile device, laptop computers were not included within the scope of this research. Furthermore, this thesis did not attempt to answer the question of whether the DOD should continue its pursuit of BYOD, but instead, was focused on the user policy and agreement, as if BYOD is inevitable.

## F. BENEFITS OF RESEARCH

It is expected that Headquarters U.S. Marine Corps, C4, Cybersecurity Division will utilize the results of this research to advance its ongoing BYOD pilot program. Additionally, it is expected that the National Security Agency (NSA) will leverage the research findings as factors to consider for future implementations in the DOD.

As stated in the USMC Mobility Strategy, "implementation of a BYOD program will allow for greater flexibility in the access, manipulation and dissemination of data from non-traditional work places to meet mission requirements."[29] This research provides the USMC with a viable user agreement to support identified technological solutions currently under evaluation, while at the same time, protecting user privacy. Furthermore, findings contained within this research will benefit broader DOD initiatives to expand mobile device solutions to include the ability to enhance the collection and dissemination of information on the battlefield. User policy and privacy concerns addressed by this research will help to ensure that the benefits of implementing a BYOD program within USMC networks will outweigh the potential risks.

## G. ORGANIZATION OF THESIS

### 1. Chapter I: Introduction

This chapter defines "mobile device" and introduces the concept and the potential benefits of a BYOD program while also providing context for this research, which seeks

[29] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 3.

to develop a viable user agreement to minimize risk to the Marine Corps enterprise network (MCEN) while protecting the privacy of BYOD participants.

### 2. Chapter II: USMC BYOD Technological Approach and Case Study Comparisons

This chapter describes the USMC'S pilot program and the BYOD technologies being evaluated. It also compares three BYOD program implementation case studies, which were utilized to identify best practices and a baseline of security controls applicable to the USMC BYOD program. Developing a baseline of controls was not the primary focus of the research, but it was necessary to understand how the various security controls could affect the content of the user agreement.

### 3. Chapter III: BYOD Case Study Privacy Concerns

This chapter defines "privacy" in the context of a BYOD program and describes the best practices and lessons learned from the same three case studies described in Chapter II to mitigate and address privacy concerns within a BYOD program.

### 4. Chapter IV: BYOD Policy Development Methodology, Considerations and Recommendations

This chapter discusses the methodology used to determine the applicable security controls for the formulation of the proposed user agreement. Recommendations and additional considerations regarding the implementation of a flexible and secure BYOD program within the USMC are also provided.

### 5. Chapter V: Conclusions, Limitations and Future Work

This chapter provides conclusions that address the research questions, the limitations encountered, and recommended future work.

### 6. Appendix A: Comparative Analysis of Case Study Organization Security Controls

This appendix provides a comparison of security controls listed within the case study BYOD user policies and the NIST Special Publication 800-53 (SP-800-53) to identify a practical baseline of security controls to address USMC security requirements.

## 7. Appendix B: Proposed Bring-Your-Own-Device User Agreement

This appendix represents the culmination of research efforts to propose a viable user agreement to support USMC BYOD implementation efforts.

# II. USMC BYOD TECHNOLOGICAL APPROACH AND CASE STUDY COMPARISONS

A BYOD program has not yet been implemented within the DOD. However, the USMC is laying the foundation for the expansion of the BYOD trend to DOD networks by running a pilot project, but various risks must be mitigated prior to BYOD becoming a reality within the DOD.[30] The primary security requirements identified by the USMC to address these risks are secure remote authentication, integrity of the mobile device OS, and control and protection of organizational networks and data.[31] NIST defines security requirements as follows:

> Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, standards, guidelines, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.[32]

In addition, NIST defines security controls as "the safeguards/ countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements."[33] Security controls can be procedure based or technology based.[34] Preferably, a security control is carried out and enforced automatically via technology. Oftentimes, however, a combination of technology and user-based procedures are required to mitigate risks to an acceptable level.

---

[30] Wyatt Kash, "Marines Break from Ranks with BYOD Test," *InformationWeek*, April 25, 2014, http://www.informationweek.com/government/mobile-and-wireless/marines-break-from-ranks-with-byod-test/d/d-id/1234840.

[31] Anderson, September 23, 2014.

[32] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Revision 4) (Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2013), B–23, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[33] Ibid., 1.

[34] Ibid., 10.

With the goal of developing a viable BYOD user agreement in support of USMC efforts, this chapter describes the efforts that were expended to identify those end-user security controls (or guidelines) necessary to address the security requirements specified previously. It is difficult to create a BYOD policy based on acceptable user behavior alone. For example, various controls should also be presented within a user agreement to inform the BYOD participants of technological capabilities that will enforce acceptable use, as well as privacy concerns, such as details regarding organizational monitoring and the conditions under which the organization will remotely perform a secure wipe of a BYOD device. Therefore, the proposed agreement provided as a result of this research includes a range of policy controls beyond just acceptable use and procedural guidelines. It was not the intent of this research to create a list of all security controls for BYOD devices, but it did require a thorough look at the current set of possibilities to provide the end user with an informed decision about participating in a BYOD program.

## A. MARINE CORPS PILOT PROGRAM

Starting in January 2015 and at the behest of the USMC, the Marine Corps Network Operations and Security Center (MCNOSC) began a four-month-long test to prove it can "deliver a secure, corporate-managed operating environment on personally owned, commercially available smartphones while also meeting the government's legal requirements."[35] To support testing, AT&T and Sprint/ViaSat provided devices, voice, and data plans.[36] These tests were originally scheduled to commence in May 2014, but have since been pushed to accommodate necessary engineering review boards and to free up the necessary resources.[37] The main purpose of this first round of tests is to identify various security issues associated with data-at-rest, data-in-transit, and the ability of the vendor-provided solutions to establish and maintain separate work and personal

[35] Wyatt Kash, "Marines Break from Ranks with BYOD Test," *InformationWeek*, April 25, 2014, http://www.informationweek.com/government/mobile-and-wireless/marines-break-from-ranks-with-byod-test/d/d-id/1234840.

[36] Robert Anderson (Chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), in discussion with the author, December 30, 2014.

[37] Ibid.

instantiations within a device.[38] Another key factor within these initial tests includes the evaluation of how derived public key infrastructure (PKI) credentials can be loaded onto a personally owned device and incorporated into the organizational container to support secure remote authentication.[39]

The two carriers only provided a total of 16 iOS and Android devices to support the testing, and although the Marine Corps plans to limit its BYOD program to these device types initially, additional device types will be allowed to participate in the future.[40] However, Microsoft devices will not likely be allowed to participate due to identified personal privacy issues associated with Microsoft's mobile OS.[41] Based on the success of this initial test, the USMC will then begin a six-month follow-on test consisting of 500 devices, which is scheduled to begin mid-2015.[42] Depending on the outcome of this pilot program, the USMC plans to make the BYOD program available to units in garrison.[43] Tactical use of personally owned devices is not authorized; thus, an alternate approach to tactical mobile devices is being sought.[44]

A description of the USMC's technological approach to implementing a BYOD program is described in the following subsections to ensure familiarity with the solutions for which the proposed user agreement is intended to support.

### 1. USMC BYOD Technology Decisions

At the time of this research, the USMC had decided on the initial vendor-provided technological solutions to be evaluated with respect to its BYOD program; however, two decisions remain: (1) which vendor solution offers the most cost effective and secure organizational instantiation on the device, as described in the next subsection; and (2) the

---

[38] Kash, "Marines Break from Ranks with BYOD Test."

[39] Ibid.

[40] Anderson, December 30, 2014.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 3.

best approach to remotely manage applications, referred to as mobile application management (MAM). The latter is a broader DOD issue to resolve, which the USMC will follow once a solution is determined, whereas the former has been narrowed to three possible solutions that will be determined during the remainder of the pilot program. It is important to emphasize that this research did not try to determine the best technological solution, but instead tried to identify the potential impact on the end user of the different approaches so that those impacts can be openly conveyed to the end user in an agreement.

### 2. Separation Solutions under Evaluation

The USMC is piloting a *container* (or sandbox) approach to separate organizational data from personal data on a device. A secure container is a separate, partitioned, and secure environment on a mobile device in which to run corporate applications and store related sensitive corporate data.[45] The USMC's BYOD container consists of a mobile application that contains a virtual private network (VPN) connector and derived certificate for authentication.[46] The challenge and concern with this approach is that the container is inherently dependent on the integrity and security of the underlying native OS. Thus, if applications can somehow bypass the OS security, or if the user can modify or replace the OS (known as *rooting* or *jailbreaking* the device), OS integrity is compromised, as is the security and separation of the personal and organizational instantiations.[47] Although rooting typically refers to an Android mobile OS, and jailbreaking refers to Apple's iOS, the concepts are similar enough that a detailed breakdown is not required to make the point, as it pertains to the potential security impacts associated with BYOD. Rooting or jailbreaking a device means that the user bypasses the manufacturer or mobile carrier security restrictions, thus elevating user privileges and access to enable the user to alter settings, install otherwise unauthorized

[45] Robert Anderson (chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), in discussion with the author, May 16, 2014.

[46] Ibid.

[47] Ibid.

third-party software and applications, as well as modify the OS and file systems.[48] The container implementations being evaluated by the USMC have root detection capabilities; therefore, it is not an unchecked vulnerability. However, the root detection capability is not 100 percent effective.[49]

AT&T's solution, called Toggle (version 4.0), creates a separate organizational instantiation on a personally owned or government furnished device. This solution is preferable to the USMC because devices can be managed from a cloud-based Toggle portal and does not require centralized mobile device management (MDM).[50] USMC administrators can log into the Toggle portal to manage users, applications, configurations, and policies, which can be set to prevent the copying or movement of organizational data to the personal side of the device and vice versa.[51] Additionally, AT&T's Toggle solution is mobile carrier agnostic and works on all common mobile device types.[52] A USMC BYOD participant will be able to download the Toggle application from the relevant application store. Registration of the device is then accomplished via an organization provided client access license, which the BYOD participant must enter into the Toggle application prior to activation.[53]

Secure Work Space is the solution offered by Blackberry. This solution is very similar to Toggle in that it is carrier agnostic and will work with most common device types.[54] However, Secure Work Space requires centralized MDM and the Blackberry enterprise infrastructure vice the purely web-based management capability associated

---

[48] Whitson Gordon, "Everything You Need to Know About Rooting Your Android Phone," *Lifehacker*, September 4, 2013, http://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone; Liane Cassavoy, "What Does It Mean to Jailbreak an iPhone?," *About Technology*, accessed June 4, 2014, http://cellphones.about.com/od/glossary/f/jailbreak_faq.htm; Souppaya, Scarfone and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 4.

[49] Ryan Fetterman (Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), email message to the author, August 26, 2014.

[50] Anderson, December 30, 2014.

[51] Ibid.; Kash, "Marines Break from Ranks with BYOD Test."

[52] Anderson, December 30, 2014.

[53] Ibid.

[54] Ibid.

with Toggle.[55] Like Toggle, Secure Work Space uses AES 256-bit encryption and meets FIPS 140-2 security requirements for cryptographic modules.[56,]

Sprint and ViaSat's joint solution is called Knox/Excide. This solution is associated with Samsung's security enhancement (SE) for Android mobile OS with additional security and management hooks provided by the ViaSat Excide technology.[57,] This solution also creates a secure organizational container on a personally owned device, offers a myriad of security options, and applies automatic security updates to the SE for Android OS to counter software bugs and malicious code or applications.[58] It is similar to a Type-1 hypervisor in that it resides below the OS on a mobile device.[59] Knox also employs a trusted boot process that works like a trusted platform module (TPM) to ensure the device is trustworthy and has not been altered.[60,] The trusted boot process works in conjunction with a TrustZone-based Integrity Measurement Architecture, which continually verifies kernel integrity.[61] Additionally, this solution has been granted the authority to operate (ATO) on sensitive DOD enterprise networks.[62] Although the most

---

[55] "Secure Work Space for iOS and Android," accessed December 30, 2014, http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/bfb/Secure-Work-Space-datasheet.pdf.

[56] National Institute of Standards and Technology (NIST), *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards (FIPS) Publication 140-2) (Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2001), http://csrc.nist.gov/publicationsfips/fips140-2/fips1402.pdf; Corsec Security, Inc., *AT&T Toggle Cryptographic Security Module, Software Version: 1.0, FIPS 140-2 Non-Proprietary Security Policy* (San Antonio, TX: AT&T Services, Inc., 2014), http://csrc nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2112.pdf; Ronen Halevy, "BlackBerry Secure Workspace for iOS & Android Gets FIPS 120-2 Certification," *BerryReview*, March 26, 2014, http://www.berryreview.com/2014/03/26/blackberry-secure-workspace-for-ios-android-gets-fips-120-2-certification/.

[57] "Technical Details," accessed December 30, 2014, https://www.samsungknox.com/en/products/knox-workspace/technical; Anderson, December 30, 2014.

[58] "Verizon Wireless Cell Phones: What Is SE Android??," accessed December 28, 2014, http://www.samsung.com/us/support/faq/FAQ00057510/75485/SCH-I545ZWAVZW.

[59] Calvin Azuri, "Samsung KNOX Hypervisor Receives Approval for Use by U.S. Department of Defense," *TMCnet.com*, March 18, 2014, http://technews.tmcnet.com/channels/enterprise-mobile-solutions/articles/373702-samsung-knox-hypervisor-receives-approval-use-us-department htm.

[60] "Technical Details"; "Trusted Platform Module (TPM) Summary," accessed December 29, 2014, http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.

[61] "Verizon Wireless Cell Phones: What Is SE Android??."

[62] Azuri, "Samsung KNOX Hypervisor Receives Approval for Use by U.S. Department of Defense."

secure solution of the three, it currently only works with Samsung devices running the SE for Android OS.

The USMC also considered another combined Sprint and ViaSat solution. This ViaSat solution is different from Excide and was delivered to the Marine Corps Systems Command for a Joint Capabilities Technology Demonstration, which is referred to as "trusted handheld" (TH2) by the vendor.[63] TH2 provides separation using a type-1 hypervisor solution, which leverages virtualization technology to partition and create separate personalities on a single device. This solution allows two instances of the mobile operating system to run in parallel, and partitions all processes and resources. One OS instance supports the personal side of the device while the other instance supports the organizational side. However, this solution has not been deemed as cost effective or practical for the USMC's BYOD program because deployment of the hypervisor to the hardware of each personally owned device is difficult to accomplish and original equipment manufacturers (OEMs) are not providing it to the general consumer base.[64]

### 3. USMC Approach to Mobile Device Management

All the solutions to data separation, as previously described, create separate work and personal instantiations within one device. To manage the enterprise instances of such mobile devices, the USMC would rather not be involved in hosting the management solution on premises and are instead leveraging industry-based cloud solutions.[65] To support this approach, the USMC has talked with commercial mobile carrier companies to develop an implementation plan that will allow the USMC to outsource the management portal as a cloud-based service, which incorporates the USMC's system security policies.[66] In this BYOD model, the management portal will be alerted if device

[63] Anderson, September 23, 2014.

[64] Anderson, December 30, 2014.

[65] Ibid.

[66] Nicole Grim, "Marine Corps Mobile Device Strategy Looks to Cut Costs," *Defense Systems*, July 26, 2013, http://defensesystems.com/Articles/2013/07/26/Marine-Corps-mobile-device-strategy.aspx?Page=1.

settings are altered or if the device is outside acceptable risk levels, and will automatically notify the USMC enterprise service helpdesk.[67]

The USMC's separation solutions under evaluation meet the security requirements for cryptographic modules set forth in the Federal Information Processing Standards (FIPS) Publication 140-2 for all cryptographic operations to provide confidentiality for data-at-rest and data-in-transit.[68,]

## B. BENEFITS OF SEPARATION

Those technical solutions that provide a separation of work and personal instances on a device provide benefits for both the employer and the employee.

Since organizational data is accessed, processed, transmitted, and stored within the organizational container, the data remains under the control of the organization. This situation creates an environment in which the user must adhere to USMC BYOD policies while utilizing the organizational container because the USMC owns that container, while allowing the user to have a different behavior when utilizing the personal container. Therefore, many common policy controls associated with employee use of organizational IT resources are inherited by and applicable to the use of the organizational container resident on an employee's personally owned mobile device. The primary employee benefit of a BYOD program is the capability for employees to gain remote access to organizational data when and where they need it. However, user behavior while working within the organizational side of a mobile device should be no different from sitting in a physical office utilizing government IT resources.

Another added benefit to the USMC is that the organizational container solution eases some of the considerations associated with legal holds and data discovery, such as subpoenas and the spillage of sensitive information. As defined by the Electronic Discovery Reference Model (EDRM), a legal hold "is a communication issued as a result of current or anticipated litigation, audit, government investigation or other such matter

---

[67] Anderson, September 23, 2014.

[68] Ibid; National Institute of Standards and Technology (NIST), *Security Requirements for Cryptographic Modules*.

that suspends the normal disposition or processing of records."[69] Furthermore, a legal hold acts as the first step in the electronic discovery process to inform employees that they must "preserve documents and electronically stored information (ESI) associated with an investigation, lawsuit, or audit."[70]

The benefit of having two instantiations or containers is that it completely separates organizational functions and data from the personal side of the device. This solution also aims to ensure user privacy as the USMC will only be able to monitor the organizational or work side of the device. In addition, if the device is lost or compromised, or if the employee leaves the organization, the organization can only delete the organization's data.

The next section describes the BYOD technology and user policy solutions adopted by three case study organizations. Additional privacy considerations and best practices identified from the following case study organizations are covered in Chapter III.

## C. CASE STUDIES

To gain a better understanding regarding how the Marine Corps' primary security requirements can be addressed through user policy, three BYOD implementation program case studies are described in this subsection. These non-DOD case study organizations have utilized different technological solutions to implement their BYOD programs; however, a comparison of each implementation and its associated user policy provides insight regarding what policies may be applicable to the USMC's BYOD user policies and technological solutions under evaluation. Despite the different technological solutions employed, numerous similarities exist between each organization's user policies. These similarities provide a base line of common controls, which can be applied to the proposed USMC BYOD user agreement as a starting point for establishing the security capabilities necessary to meet the USMC's security requirements.

---

[69] EDRM, "EDRM Metrics Glossary," accessed March 9, 2015, http://www.edrm.net/resources/glossaries/edrm-metrics.

[70] "Legal Hold," accessed January 21, 2015, http://www.symantec.com/page.jsp?id=eic-legal-hold.

To identify lessons learned and best practices regarding user policy and privacy considerations associated with BYOD implementations, two non-DOD government agencies—the Alcohol and Tobacco Tax and Trade Bureau (TTB) and Equal Employment Opportunity Commission (EEOC)—have been researched. Additionally, information from a consumer packaged goods (CPG) firm was gathered to compare practices within the private business sector. Although the firm has been extremely helpful and forthcoming regarding its BYOD program, the name of this CPG is not disclosed to support its desire to maintain anonymity and not directly disclose or associate BYOD policies and practices. From both a technology and capability standpoint, each of the case study organizations has implemented its BYOD programs differently.

The CPG's and EEOC's programs provide a basic ability to synchronize mobile devices with organizational email, contacts, calendars, and tasks, whereas TTB provides full access to network data and applications via a virtual desktop approach. These three BYOD programs differ from the solutions being evaluated by the USMC. Due to these differences, a user policy or user agreement associated with the case study organizations cannot be simply adapted or combined with any hope of addressing all the USMC's BYOD security requirements.

Appendix A provides a detailed list of the case study organizations' user policy controls and the security requirement each control supports. Within Appendix A, each case study user policy control is also mapped to the applicable NIST SP-800-53 control(s), which is discussed in more detail in Chapter IV. The following case study BYOD program descriptions focus primarily on those user policy controls and solutions that best support the three security requirements as identified by the USMC.

As a point of clarification, user agreements are commonly referred to as Rules of Behavior (RoB). For instance, both the TTB and EEOC refer to their user agreements as RoB. To avoid confusion and for the purpose of this research, they will be referred to as user agreements.

### 1. Alcohol and Tobacco Tax and Trade Bureau

The TTB has implemented a BYOD solution utilizing a Citrix virtual desktop implementation. The Citrix virtual desktop uses a small browser plugin called Citrix Receiver, which is freely available for download and turns almost any device into a thin client.[71] A thin client refers to any computer or computing device that relies on a separate computer (or server) to handle the actual computational workload. The device operating as a thin client serves only as a means to allow for user inputs via a keyboard, mouse, or touch screen, and as a means to display data through a monitor. This solution was selected because the Citrix Receiver allows the TTB to leverage established network infrastructure to create thin client devices readily and support BYOD.[72] Citrix Receiver is similar to remote desktop in that it displays and controls a virtual desktop on the user device while all the computing is done within TTB's data center. Communication is accomplished via independent computing architecture (ICA) protocol for Citrix Virtual desktop, whereas remote desktop protocol (RDP) is the protocol for remote desktop.[73] Using a virtual desktop to support BYOD allows for centralized management of the mobile devices. With respect to separation, the virtual desktop can be configured to disallow the copying of data from TTB's data center to a personal device and vice versa.[74]

Additionally, discovery in support of subpoenas can be easily conducted on a single disk array within the TTB's data center as opposed to many local hard drives dispersed throughout the country.[75] Simply stated, a user on a mobile device accesses a virtual desktop environment from a smart phone or tablet, but all data remains locked in the organizational data center. Other advantages to the TTB's implementation are that the

[71] Robert Hughes (Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau (TTB), Washington, DC), in discussion with the author, July 7, 2014.

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Ibid.

Citrix Receiver is device agnostic and runs very efficiently in limited bandwidth environments.[76]

One of the issues the TTB had to address by utilizing this technological solution was form factor. The virtual desktop creates a personal computer (PC) environment. Thus, users accessing the virtual desktop from a Mac (Apple) product must become accustomed to utilizing their Mac hardware within this PC environment. User feedback has indicated that within a couple weeks, Mac users have been able to adapt to this form factor challenge and have reacted positively.[77] This approach has also proven flexible enough to support teleworkers putting home computers on par with the systems and network environment easily, as if working in an office physically located on TTB premises.[78] Arguably, the most significant benefit to the TTB's implementation is that it allows the TTB to minimize legal considerations and the inherent delays associated with resolving issues that would otherwise require substantial legal involvement.[79]

To address the secure remote authentication requirement, the TTB utilizes two-factor authentication for all remote access.[80] Two-factor authentication to the VPN is accomplished by providing a RSA secure identification (ID) code and personal identification number (PIN).[81] Without the combination of these two factors, any attempt to establish a VPN connection is denied. This technical control is coupled with various additional policy controls to include requiring users to protect authentication credentials; reporting lost or compromised credentials; and disallowing any remote connections to TTB networks from outside of the United States.[82]

Mobile device OS integrity is a risk that the TTB has addressed through user policy, which states, "do not install or use unauthorized hardware or software…do not

[76] Hughes, July 7, 2014.

[77] Ibid.

[78] Ibid.

[79] Ibid.

[80] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy* (7320.1G) (Washington, DC: Alcohol and Tobacco Tax and Trade Bureau, 2011).

[81] Ibid.

[82] Ibid.

exchange system components…only use TTB provided and properly configured equipment and software."[83] However, the TTB has no technological solution in place to enforce the policy.[84] TTB policy requires users to install patches when available and also assigns the user the responsibility to maintain and update antivirus software.[85] This policy is required for both home computer and mobile devices used to access the TTB network. Furthermore, the policy also stipulates that if an operating system is no longer supported (e.g., Windows 98, 2000, and XP), it cannot be used to access the VPN.[86] In both home computer and mobile device cases, no scan or quarantine solution is available that looks at the connecting host devices because no solution has been identified that will work and be manageable for the TTB.[87] In short, mobile device OS integrity is the primary risk for the TTB's BYOD program.[88] A portion of the risk associated with the TTB's approach is trusting that the Citrix solution can enforce a separation policy.[89] However, the TTB believes that the potential risk to the organization's information and network is mitigated to an acceptable level via this thin client approach and the associated user agreements.[90]

Control and protection of organizational networks and data is primarily accomplished via the TTB's Citrix virtual desktop infrastructure (VDI) solution. From a personally owned device, employees can connect to the TTB network through the TTB web-based secure socket layer (SSL) VPN utilizing the two-factor authentication method previously discussed.[91] The VDI prevents users from saving any data from the TTB's

---

[83] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior* (Washington, DC: Alcohol and Tobacco Tax and Trade Bureau TTB, n.d.).

[84] Robert Hughes (Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau (TTB), Washington, DC), email message to the author, October 27, 2014.

[85] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*.

[86] Ibid.

[87] Hughes, October 27, 2014.

[88] Ibid.

[89] Robert Hughes (Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau (TTB), Washington, DC), email message to the author, December 30, 2014.

[90] Ibid.

[91] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*.

data centers to the personally owned device and vice versa. This solution ensures organizational control of data because it remains within the TTB's data centers. Additional user guidelines are identified within the TTB's user policy, some of which overlap with the controls in place to ensure secure remote authentication. The web browser on any device used to access the TTB VPN must be capable of at least 128-bit encryption and is enforced via Netscaler VPN technology.[92,] Additionally, any device not recognized as "trusted" based on proper configuration and up-to-date patches is not allowed to access the TTB network.[93] Furthermore, sensitive or PII must be encrypted prior to transmission outside of the TTB environment.[94] User policy also supports the control and protection of organizational data and networks by prohibiting employees from making any attempt to bypass these remote access or control mechanisms.[95]

Although guidelines are identified within the TTB's user policy to control and protect organizational networks and data, the TTB has very few technical capabilities to back up these policy controls. Again, the TTB has no way to monitor the configuration of devices to discern what software is on the device, and then allow or disallow a connection based on compliance with its remote access policy.[96] The TTB's technological solution only prevents the transfer of data from the organizational data centers to a personally owned device and the transfer of personal data to the organizational data centers.

### 2. U.S. Equal Employment Opportunity Commission

The EEOC refers to its BYOD program as "managed BYOD" and allows a user to synchronize a mobile device for organizational email, contacts, calendars, tasks, and open a variety of attachment formats.[97] Based on user demand, the EEOC currently supports

---

[92] Robert Hughes (Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau (TTB), Washington, DC), email message to the author, October 28, 2014; Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*.

[93] Ibid.

[94] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*.

[95] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*.

[96] Hughes, October 27, 2014.

[97] Kimberly Hancher (Chief Information Officer, Equal Employment Opportunity Commission (EEOC), Washington, DC), in discussion with the author, July 7, 2014.

only Android, Apple iOS-based and Blackberry devices.[98] If an employee chooses to participate, EEOC's administrator adds the specific device and username to the administrative console on the Globo Mobile MDM console, and the device is subsequently activated.[99] The administrator then sends an email to the user with instructions for phone setup to include the download and installation of the Globo Mobile MDM and TouchDown applications from the device's relevant app store (e.g., Apple's App Store for iOS, Google Play for Android, etc.) and identifies specific settings that must be established prior to synchronization.[100] Proper device configuration is validated via the MDM administrative console.[101] This process serves two purposes. First, it correlates the participant to a specific personally owned device, and second, it serves as a form of network access control (NAC). The NAC consists of protocols put in place to check the configuration and security of an endpoint device when it is initially connected to a network. Although the device can only be utilized to access limited resources within the EEOC enterprise (i.e., the exchange server), the NAC does verify the endpoint device matches the intended user and is properly configured prior to allowing access to EEOC enterprise services.

Since unlimited remote access to the EEOC data centers is not allowed for standard BYOD participants, the primary security requirement in this case is control and protection of organizational data accessible via EEOC enterprise services (i.e., email). The EEOC provides two methods for employees to access organizational email and calendar services. The first is web-based access to GroupWise, while the second option is the use of an organizational container application.[102] For web-based access, organizational emails are accessed via a web browser and Internet connection. In this

---

[98] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*, U.S. Equal Employment Opportunity Commission (EEOC) fv1c (Washington, DC: U.S. Equal Employment Opportunity Commission, 2012).

[99] Kimberly Hancher (Chief Information Officer, Equal Employment Opportunity Commission (EEOC), Washington, DC), in discussion with the author, October 31, 2014.

[100] Ibid; J. Scott Walker, (Enterprise Sales Manager, Globo Mobile Technologies Inc., Palo Alto, CA), in discussion with the author, December 15, 2014.

[101] Walker, December 15, 2014.

[102] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

instance, emails and associated attachments are not downloaded by default to the personally owned device.[103] However, no technical controls are in place to prevent a user from inadvertently or intentionally downloading organizational information and attachments to a personally owned device. This being the case, the EEOC must rely on the user's adherence to policy to protect organizational information accessed via GroupWise. For example, the EEOC's user policy stipulates that although the "user will not download or transfer sensitive business data to their personal devices…participants must routinely delete any sensitive business files that may be present on the device as a result of an inadvertent download."[104]

The second option for accessing EEOC services is through a container application, which provides the capability to control organizational data. The EEOC utilizes TouchDown as its container solution to separate the personal side of the device from organizational emails, downloaded attachments, contacts, calendars, and tasks.[105] Organizational emails and attachments are downloaded and stored on the personally owned device, but remain within the TouchDown container. Additionally, this container solution allows the EEOC to conduct a selective remote wipe of only the organizational data vice a complete wipe of the device.[106] TouchDown employs advanced encryption standard (AES) 256-bit encryption to protect data-at-rest within the container and prevents the movement of data from the organizational container to the personal side of the device and vice versa.[107] Assuming a BYOD participant adheres to the user policies when utilizing the web-based access option, and only utilizes the TouchDown container to download organizational data; the organizational data is effectively controlled and protected. As an added layer of protection and control of organizational data, BYOD

[103] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[104] Ibid.

[105] Hancher, October 31, 2014.

[106] Walker, December 15, 2014.

[107] James Randle (Information Technology Specialist, Equal Employment Opportunity Commission (EEOC), Washington, DC), in discussion with the author, December 16, 2014.

participants must agree that the personally owned device will not be shared with anyone else to include family members.[108]

To participate in EEOC's BYOD program, participants must use a properly configured device based on EEOC defined security settings and an associated password that then grants permission to use EEOC services.[109] The password is enforced through the MDM solution and is required to gain access to the device, but no subsequent passwords are required once access to the device is achieved.[110] Globo Mobile serves as EEOC's MDM solution and employs technical capabilities to prevent misconfigured devices from using EEOC services.[111] Through the MDM, the EEOC maintains the ability to conduct a selective remote wipe or a full wipe on a device if it is reported lost or stolen. Remote wipes are initiated and subsequently confirmed via the MDM administrative console.[112] Additionally, all organizational email and data resident within the TouchDown container will be automatically deleted following 25 failed password attempts.[113] Remote wipes are also conducted on devices removed or transferred out of the BYOD program.[114] Whether lost, stolen, or transferred, the devices are also removed from the MDM console.[115] It is important to note that remote wipes are not a reliable security control because an attacker can access information stored on a device before it is wiped.[116] Thieves can potentially bypass logical access controls or steal an unlocked device. Thieves are also quick to disallow connectivity to the device by placing it in airplane mode, putting it in a box or bag that makes it impossible to receive the remote

---

[108] Randle, December 16, 2014.

[109] Hancher, July 7, 2014.

[110] Hancher, October 31, 2014.

[111] Ibid.

[112] Walker, December 15, 2014.

[113] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[114] Hancher, October 31, 2014.

[115] Ibid.

[116] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 9.

wipe signal, or simply turn it off until the resident data can be exploited at a later time.[117] Additionally, BYOD participants may not realize the device is lost for several hours or may wait days to report a lost or stolen device, which creates a window of vulnerability for organizational data.[118] Still, the ability to initiate remote wipes is an important additional layer of protection for organizational data.[119] However, from the user point of view, the ability to wipe personal data and applications remotely may be alarming, and result in a lower BYOD acceptance than anticipated.

In addition to detection technology, the EEOC also addresses personally owned mobile device OS integrity through a user policy that prohibits participants from installing unauthorized third-party software or attempting to jailbreak the device.[120] Policies are set within the MDM administrative console for application management.[121] If EEOC BYOD participants download an unauthorized application to their personally owned device or attempts to remove required applications, an alert is sent to EEOC administrators or directly to the participants notifying them that if not corrected, the ability to continue BYOD privileges will be terminated.[122] Policy also assigns users the responsibility to apply patches and updates in a timely fashion to maintain an up-to-date defensive posture.[123] MDM technical solutions support these user policy controls by maintaining the capability to identify and prevent the use of EEOC services for devices not within standards.[124]

---

[117] Tom Kaneshige "Is a Remote-Wipe Policy a Crude Approach to BYOD Security?," *CIO*, September 16, 2014, http://www.cio.com/article/2683902/byod/is-a-remote-wipe-policy-a-crude-approach-to-byod-security.html.

[118] Ibid.

[119] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 9.

[120] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[121] Walker, December 15, 2014.

[122] Ibid.

[123] Ibid.

[124] Hancher, October 31, 2014.

In addition to the more general Globo Mobile solution, a VPN connection to access EEOC's network is provided to a limited number of privileged users primarily consisting of executive level leadership and is approved on a case-by-case basis by the chief information officer (CIO).[125] The number of privileged users is small enough that monitoring is limited to identifying rogue device access.[126] The EEOC only allows personally owned iOS devices to establish VPN connections. EEOC BYOD administrators manually monitor rogue devices by looking for non-iOS devices or devices that do not correlate to a specific user authorized to establish a VPN connection.[127] The MDM is not involved with any aspect of the EEOC's VPN remote access solution.

Those senior executives allowed to establish VPN connections with personally owned iOS devices must receive additional mobile device awareness training and can only use EEOC approved and configured Cisco VPN client software.[128] To establish these connections and support secure remote authentication, EEOC administrators must be allowed to install mobile device management tools, as well as an anti-virus security suite—that consists of a firewall, anti-virus software, and website protector applications—on the personal device.[129] A second username and password, in addition to the initial device access password, is also required for remote authentication.[130]

### 3. Consumer Packaged Goods Firm

Since only a limited number of government BYOD implementations have been established, a private sector program, which has requested anonymity, has also been included in this research. All interviews were conducted in confidentiality, and the names

---

[125] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[126] Hancher, July 7, 2014.

[127] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[128] Hancher, October 31, 2014.

[129] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[130] Hancher, October 31, 2014.

of interviewees are withheld by mutual agreement. According to the company's website accessed on August 11, 2014, this CPG is one of the world's leading food manufacturers, and is well known for a myriad of products. The CPG's BYOD program is similar to the EEOC's program in that it provides employees the ability to synchronize corporate email, calendars, contacts and notes, and does not allow participants full access to corporate data centers.[131] The CPG's implementation of BYOD also allows for the utilization of Microsoft Lync to support instant messaging.[132] Remote access to the CPG's corporate data centers is only allowed using corporate furnished equipment consisting of iOS products that will not be described further in this thesis, as it falls outside the bounds of a BYOD program.

Based on discussions with a company representative, the CPG utilizes MobileIron as its MDM solution to support BYOD, which is downloaded to employee devices from relevant vendor application stores and is available for most of the common mobile device types.[133] The user then registers the device with the corporate MobileIron account. After an employee requests to participate in the BYOD program, the employee reads and agrees to the CPG's user policy, downloads the MobileIron application, and is ready to work; a relatively simple and streamlined process.[134] Like EEOC, this process correlates a CPG participant to a specific personally owned device.

Similar to the EEOC's BYOD program for standard users, the CPG allows limited access to enterprise resources (i.e., exchange servers) from a personally owned device.[135] To address the security requirement for control and protection of organizational data, the CPG user policy stipulates that the user can only backup corporate data to a corporate device.[136] Therefore, BYOD participants must exercise caution when conducting a

[131] Management Information Systems Director and Chief Information Officer, company name withheld upon request, in discussion with the author, July 17, 2014.

[132] Ibid.

[133] Ibid.

[134] Ibid.

[135] Ibid.

[136] Consumer Packaged Goods (CPG) Firm Representative, email message to the author, July 24, 2014.

backup of personal data resident on their device to a home computer or another personally owned device to ensure company data is not also transferred to a non-organizational device. The CPG does not have any technological controls in place to prevent the backup of corporate data to non-corporate devices, and is therefore, based solely on user adherence to policy.[137] The CPG policy requires that sensitive company data present on a personally owned device must be encrypted and password protected, and participants must agree to periodically delete any unnecessary information stored on the device.[138] Furthermore, backing up corporate data to third-party file sharing and Internet backup services, such as iCloud and Dropbox, is prohibited.[139] Operational security (OPSEC) principles are also addressed through user policy and warn participants that separate pieces of information can be consolidated to create a detailed picture of sensitive activities.[140] The CPG has not implemented technological solutions to create separate work and personal instantiations, and thus, cannot prevent the commingling of organizational and personal data.[141]

The CPG's user policy stipulates that employees must let the company know immediately if a device is lost or stolen, at which point the CPG can leverage MobileIron to wipe the device remotely.[142] Personally owned devices will also be wiped following 10 unsuccessful attempts to access the device.[143] If an employee separates from the CPG, the company service desk will initiate a remote wipe of the personally owned device, but will seek to delete only company data.[144] However, because the CPG is not utilizing a container approach to separate personal and organizational data, conducting a selective wipe will prove challenging. For this reason, the CPG includes verbiage within its user policy to inform BYOD participants, "personal information stored on your personally

[137] CPG Representative, July 17, 2014.

[138] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Ibid.

[143] Ibid.

[144] Ibid.

owned device might be permanently lost or made unavailable due to a wipe of the device…"[145]

The CPG's policy further forbids the download or installation of unauthorized third-party software and will quarantine any device with non-standard add-ins to unlock or jailbreak the device.[146] To enforce this control, the CPG's MDM solution has the capability to detect unauthorized software. Although this control is stated in the CPG user policy, in actuality, the CPG does not manage or restrict applications that an associate might install on his personally owned device.[147] Instead, the CPG relies on a "user responsibility principle" (e.g., users must be responsible for their systems and the ability to perform their jobs with the provided tools).[148] However, technical solutions are in place through the MDM to identify improperly configured devices, as well as devices with a compromised OS.[149] The detection of configuration changes occurs on the device via the MobileIron application, which periodically synchronizes to the MobileIron administrative console.[150] Any alterations to the device are simultaneously passed to the administrative console during these periodic communications, which subsequently alert the CPG BYOD administrators and the participant if a device is outside of acceptable parameters.[151] Furthermore, only BYOD administrators can remove the MDM application from a personally owned device.[152]

Although the CPG does not utilize the full container capabilities offered by MobileIron, the MobileIron MDM application itself has jailbreak detection

---

[145] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[146] Ibid.

[147] Consumer Packaged Goods (CPG) Firm Representative, email message to the author, January 8, 2015.

[148] Ibid.

[149] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[150] Alexander Mead (Federal Inside Sales, MobileIron, Mountain View, CA), in discussion with the author, December 23, 2014.

[151] Ibid.

[152] Ibid.

capabilities.[153] In this case, if the user successfully jailbreaks the device, the MobileIron application will immediately detect the OS alterations and automatically remove all local copies of organizational data within the MDM container application, which essentially wipes the device of all corporate information without a connection to the MDM administrative console.[154] Once a connection to the administrative console is re-established, further security measures can be taken depending on the organization's established security policies.[155] However, because the CPG is not utilizing the full capabilities offered by MobileIron, this automatic removal of organizational data resident on the device would not be accomplished. Instead, the CPG relies on a wireless connection to the device, and if a participant alters or disables the CPG prescribed settings, the participant's service to the personally owned device will be suspended and a full remote wipe will be executed.[156] Remote wipes initiated via the CPG's MobileIron MDM solution are susceptible to the same connectivity issues as those discussed in the EEOC section. Like the EEOC, the CPG assigns the responsibility for applying software updates and security patches to the user.[157]

The CPG user policy emphasizes physical protection of the device. For example, policy guidance directs users to never leave mobile devices in a vehicle nor include devices with checked luggage.[158] Additionally, if a local government or outside agency seizes a participant's device, the device must be inspected by the organization prior to continuing its use to process or access company data.[159] To find a lost device, the CPG policy also stipulates that the user must leave location services turned on.[160]

---

[153] Alexander Mead (Federal Inside Sales, MobileIron, Mountain View, CA), email message to the author, December 29, 2014.

[154] Ibid.

[155] Ibid.

[156] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[157] Ibid.

[158] Ibid.

[159] Ibid.

[160] Ibid.

## D. CASE STUDY COMPARISON TO SUPPORT USMC SECURITY REQUIREMENTS

This section compares the technical and policy controls established by the three case study organizations. Although each organization has adopted numerous additional user and technical controls, this section focuses on those controls most relevant to supporting the three primary security requirements identified by the USMC, which are secure remote authentication, OS integrity, and control and protection of organizational data and networks.

### 1. Security Requirement—Secure Remote Authentication

The TTB is the only case study organization that allows access to its data centers for all BYOD participants. Although the EEOC does allow VPN connections to the organizational network, this access is limited to a small group of privileged users. Controls common among these two case study organizations to support secure remote authentication include at least one-factor authentication. The TTB requires two-factor authentication via a RSA ID and PIN. The EEOC's requirement to first register a device to ensure it correlates to a specific user, as well as the installation of various configuration software, does provide a level of added protection, but it still relies on a single factor for remote authentication.[161,] Although the EEOC employs one-factor authentication, one password is required to initially access the device, and a separate second username and password is required to establish a VPN connection.[162] The ability to identify whether a device is authorized access to EEOC data centers must be accomplished manually, which makes it probable that an unauthorized access, however unlikely, will only be discovered after the fact. The CPG only allows VPN connections to its corporate data centers using corporate furnished equipment consisting of iOS products. Since the CPG's BYOD approach only allows limited access to enterprise services, a comparison of its remote authentication practices is not discussed. However, the CPG does require a 4-digit PIN for logical access to a personally owned device used

[161] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*; U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[162] Ibid.

within its BYOD program, and enforces this requirement through the MDM application.[163]

### 2. Security Requirement—OS Integrity

The EEOC and the CPG use a centralized MDM approach to monitor personally owned mobile devices to ensure proper configuration and OS integrity. Both MDM solutions maintain the capability to manage applications, can see when unauthorized applications have been installed, and when required applications have been removed. Furthermore, the MDMs can detect devices outside of organizational defined risk parameters and will quarantine these devices to deny continued access to enterprise services. The CPG takes this a step further by initiating a remote wipe of the devices with improper configuration settings or a compromised OS.[164] The TTB recognizes mobile OS integrity as a risk within its BYOD program, but has not identified a manageable technological solution to monitor or counter this vulnerability.[165] However, the TTB's thin client approach to BYOD does reduce the potential harm associated with this vulnerability. All three case study organizations require users to keep the original OS current by applying patches and security updates when available.[166]

Although the aforementioned controls are all technical approaches employed to either prevent or detect a compromised OS, no measurement for how much confidence should be placed on such approaches actually exists because none have been submitted to a third-party evaluation of their capabilities, such as an evaluation against the Common Criteria framework.[167] Dependence on these approaches for OS integrity, therefore, carries some amount of risk.

---

[163] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[164] Ibid.

[165] Hughes, October 27, 2014.

[166] Alcohol and Tobacco Tax and Trade Bureau, *Remote Access Policy*; U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, August 13, 2014.

[167] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCIMB-2012-09-[001, 002, 003] Common Criteria Project Sponsoring Organizations, January 2012.

### 3. Security Requirement—Control and Protection of Organizational Data and Networks

All three case study organizations use several common controls that would meet the USMC requirement to control and protect organizational data and networks. A password or PIN is required to access logically any personally owned device used within EEOC's and the CPG's BYOD programs.[168] For data-at-rest, EEOC's organizational container utilizes AES 256-bit encryption; however, complete device encryption is not required.[169] It is worth noting, however, that iOS and the new Android OS provide full device encryption by default utilizing AES 256 and AES 128-bit encryption, respectively.[170] When used to handle sensitive information, the CPG requires the use of encryption for personally owned devices.[171] The EEOC and the CPG also maintain the capability to initiate a remote wipe of personally owned devices.[172] Since TTB's technological solution ensures that organizational data is not stored on a personally owned device, this concern is well mitigated and the capability to remote wipe a device is not required.

TTB, EEOC and the CPG policies have controls in place that either prohibit the download of sensitive organizational data and PII to a personally owned device or requires such organizational data present on the device to be encrypted.[173] The EEOC and the CPG further require users to delete organizational information periodically that

---

[168] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[169] Randle, December 16, 2014.

[170] Robert Sheldon, "How iOS Encryption and Data Protection Work," *techtarget.com*, February 2013, http://searchconsumerization.techtarget.com/tip/How-iOS-encryption-and-Data-Protection-work; "Encryption," accessed December 20, 2014, https://source.android.com/devices/tech/security/encryption/Android; Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police," *The Washington Post*, September 18, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[171] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[172] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[173] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*; U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

may have been inadvertently downloaded or is no longer needed.[174] Unauthorized disclosure is also addressed in both TTB's and the CPG's user policies, and advises participants to exercise caution when using social networking and email services.[175]

All three case study organizations clearly state in user policy that users are prohibited from downloading or installing unauthorized software; however, only the EEOC and the CPG—through their respective MDMs—have the technological solution in place to enforce the policy or detect violations.[176]

As for the protection of data-in-transit, only the TTB clearly states in its user policy that sensitive organizational data must be encrypted prior to transmission outside of the TTB environment.[177] The EEOC utilizes the proprietary GroupWise encryption for internal traffic, which is sufficient, as long as traffic remains within the GroupWise environment and is not downloaded to the personal side of a device.[178] The CPG addresses the transmission of sensitive data through user policy and warns participants to exercise caution when utilizing distribution lists or when forwarding emails to ensure only individuals with a need-to-know are allowed to view sensitive information.[179] Moreover, the CPG forbids the backup of corporate data to Internet cloud services.[180] Both the EEOC's and the CPG's user policies limit the backup of organizational data to only organizationally owned devices.[181] Other than the authorized devices described in each case study organization's respective programs, the TTB and EEOC have user policy

---

[174] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[175] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*.

[176] Consumer Packaged Goods (CPG) Firm Representative, email message to the author, August 13, 2014; U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[177] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*.

[178] Randle, December 16, 2014; Novell, "Native GroupWise Encryption, GroupWise 6.5 Administration Guide," accessed December 18, 2014, http://www.novell.com/documentation/gw65/?page=/documentation/gw65/gw65_admin/data/ak9e3ev.htm.

[179] Consumer Packaged Goods (CPG) Firm Representative, email message to the author, August 13, 2014.

[180] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[181] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

guidelines in place to control the physical connection of privately owned devices to the organizational network and systems. The TTB clearly states that privately owned equipment will not be connected to TTB systems or networks.[182] Whereas, the EEOC only allows BYODs with FIPS 140-2 encryption capabilities (only BlackBerry devices per EEOC current policy) to be connected to organizational PCs.[183] Both the TTB and the CPG have user policy controls in place regarding physical protection of personally owned devices; however, the CPG stresses this point in the most depth.[184] Finally, prompt reporting of lost, stolen, or potentially compromised devices and associated credentials is required by all case study organizations.[185]

Unauthorized disclosure of sensitive government information, as well as the spillage of classified information onto personally owned mobile devices, is another area of concern for the USMC. Although none of the case study organizations covered in this chapter works with classified information, their BYOD programs do address concerns associated with the unauthorized disclosure of sensitive organizational data through policy. Technical controls previously identified can provide limited response mechanisms, but are still inadequate to protect classified information. Additionally, these controls often involve operator intervention and comprise only one facet of an organization's incident response plan. Both the TTB and the CPG policies state that users must notify their respective information security representatives if an unauthorized disclosure or related information security issue is suspected.[186] Technical controls to prevent or detect the spillage of classified information within the USMC's BYOD program are nonexistent, and must therefore, be addressed through policy (such as a prohibition on the use of a device for classified data) and prompt reporting requirements so that appropriate action can be taken.

---

[182] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*.

[183] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[184] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[185] Ibid.; U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[186] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, August 13, 2014.

All three BYOD programs researched are voluntary with no expectation for employee reimbursement. As mentioned, few technological similarities exist between the BYOD implementations researched when compared to the technological solutions being evaluated by the USMC. Therefore, each organization has implemented different compensating user policy security controls based on these technological differences. For this reason, the user policies and agreements developed by the TTB, the EEOC and the CPG cannot be simply compiled to create a comprehensive user policy for the USMC's BYOD program. Best practices and commonalities to these BYOD program user policies can, however, be leveraged as a starting point for establishing a viable user agreement for the USMC. Additional stipulations and considerations are required to ensure adherence to DOD policies while also tailoring the standards to suit the USMC's technological solutions being considered.

Personal privacy associated with the use of a personally owned device is the key concern for BYOD participants. Striking the proper balance of personal privacy within a BYOD program helps ensure that both the organization and participant can benefit from the flexibility a BYOD program provides. Therefore, privacy considerations for each case study organization have also been reviewed as described in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. BYOD PRIVACY

## A. BYOD PRIVACY DEFINED

Two fundamental issues within a BYOD program are privacy and the protections available when using a personally owned device in a dual use scenario. An organization must not only ensure that the device can securely manage organizational information, but that safeguards are in place for the personal information residing on a device, not just from those *outside* the organization, but from those managing the device *within* the organization itself. Protection of a user's privacy is driven by good policy that clearly outlines any potential privacy concerns, all while guaranteeing that a user's expectation of privacy is preserved. This situation can be especially challenging because no two organizations will have the same information protection policies based on differing missions and risk tolerances. Additionally, no two users will view privacy the same because of differing life goals, life experiences, and risk tolerances. As a result, it is imperative that organizations provide an appropriate level of both security and privacy.

It is necessary to define the meaning of privacy with respect to this research because it can be considered by many to be a contested concept. According to NIST SP-800-53, "Privacy involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared."[187] The NIST SP-800-53 also states, "Privacy is more than security, however, and includes, for example, the principles of transparency, notice, and choice."[188] These definitions provide a baseline for what rights a user should be afforded and approach privacy more from an individual perspective, as well as stress that it is the individual's right to decide what or how much personal information to share. Additionally, they offer organizations implementing a BYOD program with considerations that must be recognized when a dual use device contains or is accessing both personal and corporate data.

---

[187] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, J–1.

[188] Ibid.

Evaluation of various definitions regarding privacy found that the NIST SP-800-53r4 best captures privacy as it relates to a BYOD program. This conclusion was based on two critical factors and did not consider any technological solutions that could separate personal and corporate data on a device. First, a BYOD program should be completely voluntary. An employee should have the right to choose not to participate or opt out of a BYOD program if the privacy concerns or other terms and conditions are deemed unacceptable. Second, a BYOD program should correctly set the users' expectation of privacy in a BYOD environment. Prior to an enrollment in a BYOD program, users should understand the potential privacy concerns associated with accessing corporate data on a personally owned device. Users must also recognize that some BYOD programs require them to consent to terms that may include monitoring or other actions that could lower their expectation of privacy on a personally owned device. As a result, users accepting these terms must realize the privacy rights that they are surrendering as a result of enrolling in the BYOD program.

## B. CASE STUDIES

To identify potential privacy considerations that exist within different BYOD programs, research was conducted on current policies and practices from two non-DOD government agencies and one commercial sector entity as outlined in Chapter II. The information gathered provided lessons learned with respect to privacy, as well as insight into how the different organizations have overcome concerns pertaining to the protection of user privacy. Additionally, the case studies offer potential implementation models for the USMC to consider throughout the testing phase of their BYOD pilot program.

As discussed in Chapter II, the ways that the CPG firm, the EEOC, and the TTB have implemented their BYOD programs differ. This distinction is important to note because regardless of how their programs were implemented, organizations need to understand that by statute, employees are entitled to a reasonable expectation of privacy.[189]

[189] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions,* 13.

### 1. Alcohol and Tobacco Tax and Trade Bureau

To overcome potential privacy concerns within its BYOD program, the TTB has implemented a technological solution that utilizes virtualization. As previously discussed, the virtualization technology completely isolates TTB's corporate data from the personal user data residing on a device. This concept is important to note from a privacy perspective because it highlights that TTB's data is not stored on the personally owned device and no work-related computation is directly performed on the BYOD hardware.[190] Information within TTB's data center remains resident to the data center, which restricts users from copying data from the enterprise to the device and vice versa. The personally owned device functions no differently from a normal smartphone or tablet that allows users access to all their personal or private information that resides on the device. Additionally, this solution guarantees that users' privacy is protected knowing that the TTB has no ability or need to access the device.

The technological solution that the TTB has implemented within its BYOD program serves as an example of how potential privacy concerns on the personal side of a device can be mitigated. Furthermore, the virtualization enables the TTB to only manage and monitor its data. Another important aspect of the TTB's BYOD program is that it is completely voluntary. As a result, its policy mandates that interested employees sign a user agreement prior to enrollment. The user agreement applies only to the corporate accessed data and acts as a legal agreement between the TTB and its BYOD users. Signing the user agreement means that employees acknowledge that the "Use of the TTB systems constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities."[191] The employees' consent to the aforementioned terms eliminates their expectation of privacy when they utilize the virtual desktop to access corporate data and grants the TTB the authority to conduct the necessary actions to ensure its corporate data is controlled and protected.

---

[190] "Bring Your Own Device, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs."

[191] Alcohol and Tobacco Tax and Trade Bureau, *TTB IT Security Rules of Behavior*.

### 2. U.S. Equal Employment Opportunity Commission

The EEOC's managed BYOD program, like the TTB's program, also employs a technological solution to control and protect organizational data. However, these solutions are not the same and accordingly require different policy considerations to address user privacy concerns. The EEOC leverages a MDM tool provided by Globo Mobile that allows the EEOC to easily manage and enforce its security policies on registered devices.[192] As discussed in Chapter II, the EEOC also provides two methods for employees to access EEOC enterprise services, web-based access to GroupWise and an organizational container application.[193] Although both methods provide registered EEOC employees with an easy way to access corporate data on a personally owned device, user privacy concerns that exist when accessing data through the container application differ from those of GroupWise. As previously discussed, the EEOC utilizes TouchDown as its container solution to separate the personal side of the device from EEOC enterprise services.[194] Enterprise services accessed through TouchDown remain resident to the secure container, which prevents the movement of data from the organizational container to the personal side of the device and vice versa.[195] This solution mitigates user privacy concerns by ensuring that corporate data never resides on the personal side of the device. Furthermore, the container solution allows the EEOC to control organizational data without accessing the personal side of the device, which maintains the user's privacy.

The alternative method of accessing EEOC enterprise services through web-based access to GroupWise does not create a separate secure container. Since no technical controls are in place that prevents employees from downloading organizational data when utilizing GroupWise to access EEOC services, the potential exists for the commingling of organizational and personal data on a personally owned device. This concern is discussed

---

[192] Hancher, October 31, 2014.

[193] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[194] Hancher, October 31, 2014.

[195] Randle, December 16, 2014.

in Chapter II; however, it is important to revisit it based on the potential privacy issues that could arise by having organizational data on the personal side of a device. On the surface, it appears as a security issue for the organization, not a privacy concern for the employee. However, if the organization learns that an employee has violated this policy, then the organization will enforce its right (as described in EEOC's user policy) to look at all the data on the personal side of the device to verify that all organizational data has been removed, which could result in a loss of privacy with respect to the user's data. EEOC's user agreement specifically states, "Users will not download or transfer sensitive business data to their personal device."[196] To ensure that their data is protected, the BYOD participants in the EEOC's organization are required to read, acknowledge, and adhere to the user agreement prior to enrolling. Additionally, employees who accept the terms of enrollment are subject to administrative, disciplinary, or legal actions if found to be noncompliant or in violation of the policy or user agreement.[197]

Another privacy concern that the EEOC recognizes within its user agreement also stems from the potential for commingling of organizational and personal data on a personally owned device. To set a user's expectation of privacy appropriately, EEOC includes an "Expectation of Privacy" notice within its user agreement.[198] This notice informs the user, "EEOC will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls… or to respond to legitimate discovery requests arriving out of administrative, civil, or criminal proceedings."[199] Although the notice only applies to users who download corporate data to their personal device via GroupWise, it helps to reinforce the aforementioned organizational policy against downloading organizational data to a personal device.[200] While the EEOC respects the users' privacy, this notice informs them that if they choose

---

[196] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[197] Ibid.

[198] Ibid.

[199] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[200] Ibid.

not to adhere to policy, the EEOC, under certain circumstances, can rightfully gain access to the personal device to ensure the protection of corporate data.

Since the BYOD program is voluntary, if users at any time decide they do not want to comply with the requirements outlined in the user agreement or find the requirements too burdensome, they may opt out of the BYOD program.[201] In such instances, the EEOC will suspend the employees' ability to synchronize to enterprise resources and conduct a selective wipe of the organizational container.[202] The selective wipe by design only erases data residing in the container and does not affect any personal data outside of the container. This process ensures that organizational data is protected and preserves the users' privacy on the personal side of the device. The above-mentioned BYOD policy controls implemented by the EEOC help to protect the organization from potential user privacy concerns and illustrate how reliant the organization is on strict participant adherence to user policy to mitigate these concerns.

### 3. Consumer Packaged Goods Firm

The CPG is similar to the EEOC in that it too employs a MDM solution that allows it to manage and enforce its security policies easily on registered devices. Additionally, the CPG's BYOD program, like the EEOC's program, provides employees the ability to synchronize to corporate email, calendars, contacts, and notes on their personally owned device.[203] The CPG, however, has not implemented a container solution, and as a result, many of the user privacy concerns that exist for EEOC employees accessing enterprise services through GroupWise also exist for employees accessing the CPG's corporate data. As no technical controls are in place to separate organizational data from the personal side of the device, the potential exists for the commingling of organizational and personal data on an employee's personally owned device. To address this issue, the CPG, like the EEOC, relies on strict participant adherence to user policy to mitigate potential organizational and user privacy concerns.

---

[201] Hancher, October 31, 2014.

[202] Ibid.

[203] CPG Representative, July 17, 2014.

To ensure that BYOD participants are aware of potential constraints that may exist when using their mobile device as dual use, the CPG requires employees to read, acknowledge, and adhere to the user agreement prior to enrolling. The user agreement outlines the company's policy and defines what is perceived as acceptable use when storing and processing company data on a personally owned device.[204] Moreover, the user agreement serves as a voluntary contract between the employee and the organization, which permits the CPG to restrict or revoke access if the policy is violated.[205] In addition to defining acceptable use, the CPG provides supplemental controls and notifications within its BYOD policy that attempt to address user privacy concerns.

One such supplementary control addressing a user privacy concern is highlighted in the "Intellectual Property Restrictions" section of the company policy.[206] This section informs the user, "All material that passes through the Company network or that is stored on Mobile Devices—including personally owned Mobile Devices—for the purpose of conducting business belongs to the Company."[207] Additionally, it states, "This material is subject to the Company ownership, confidentiality and use restrictions that apply."[208] Although this control does not stipulate that the company will arbitrarily access the personal side of the device, it serves as a reminder to the user that organizational data belongs to the company, and if needed, the CPG can and will access the device to ensure that its data is protected. This control is also highlighted in the "Privacy" section of the CPG's "Appropriate Use of Electronic Media Policy," which supports the overall company policy of acceptable use by again stressing that any organizational data stored on personal devices is the property of the CPG.[209] Although legal aspects are associated with accessing an employee's personal device without the employee's knowledge or consent, they fall outside the scope of this research. Still, the CPG has taken steps

[204] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[205] Ibid.

[206] Ibid.

[207] Ibid.

[208] Ibid.

[209] Consumer Packaged Goods (CPG) Firm Representative, August 13, 2014.

through policy to minimize the need to access an employee's personal device by clearly identifying what constitutes acceptable use and defining it in the user agreement.

Several additional user policy issues that the CPG has worked to overcome also stem from employee privacy concerns. In the case of data discovery, the CPG user policy identifies the possibility of a legal hold on the mobile device to conduct the data discovery.[210] Some employees have interpreted this legal hold to mean that the company will take custody of the dual use device for an indefinite period of time. In actuality, the CPG will seize the device just long enough to make a copy of the data it contains before returning it to the owner.[211] Several CPG employees have also expressed skepticism regarding remote wipes.[212] The CPG user policy stipulates that employees must let the company know immediately if their device is lost or stolen, at which point the CPG can leverage MobileIron to wipe the device remotely.[213] In this case, confusion can arise regarding what constitutes "immediately," especially if the owners does not know if they dropped it at the airport or simply left it at a friend's house. Since the CPG has not implemented technological solutions to create separate work and personal instantiations, it cannot prevent the possible commingling of organization and personal data. This being the case, the entire device must be wiped if lost or stolen. The last stipulation that has required clarification is that the user must leave location services turned on.[214] The CPG clearly states within its user policy that this will only be used to find a lost device; however, employees have voiced concerns that the company might use it to track their activities.[215] The potential to track a user's location is a significant concern to sales personnel and others with roles involving travel.[216]

---

[210] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[211] CPG Representative, July 17, 2014.

[212] Ibid.

[213] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[214] Ibid.

[215] Ibid.

[216] CPG Representative, July 17, 2014.

As both the EEOC's web-based access to GroupWise and the CPG have no technological solution in place to provide for the separation between organizational and personal use of the device, their policies state that should a remote wipe be required, the organization will seek to only delete organizational email or company data, respectively.[217] Although not specifically stated in either the EEOC's or the CPG's policy, because the possibility exists that organizational data can be commingled with personal data, the entire device may need to be wiped. Additionally, both policies state that in the event of a legal hold, the organization may need to access all data stored on the personally owned device.[218] In the case of the EEOC, this practice is only applicable if a BYOD user does not adhere to policy, such as downloading government email, attachments, or documents to the personal device.[219] The CPG policy clearly states that privacy cannot be assured, and although it is not explicitly stated in the EEOC's policy, the same can be reasonably inferred.[220]

The three highlighted case studies demonstrate that user privacy is a major concern when implementing a BYOD program. Additionally, they illustrate how organizations can and have overcome potential privacy concerns that arise when allowing a personally owned device access to organizational data. While many of these concerns can be mitigated through technological solutions, a well-developed policy outlining additional compensating security controls can also ensure that these concerns are alleviated.

## C. UNITED STATES MARINE CORPS

Recognizing that user privacy plays a significant role in any BYOD program, the USMC identified privacy as one of the factors that led it to implementing a technological solution utilizing containerization. The container solution under evaluation by the USMC

---

[217] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*; Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

[218] Ibid.

[219] U.S. Equal Employment Opportunity Commission, *Bring Your Own Device—Policy and Rules of Behavior*.

[220] Consumer Packaged Goods (CPG) Firm Representative, July 24, 2014.

creates a separate secure organizational instantiation on a personally owned device and aligns with the type of solution recommended in NIST SP 800-124, which states, "The client application and data should be sandboxed from the rest of the device's applications and data in a secure container, both helping to protect the enterprise from a compromised device and helping to preserve the privacy of the device's owner."[221] The separation that a container solution provides enhances privacy as compared to previously discussed EEOC and CPG BYOD technological solutions, so that the USMC BYOD user privacy concerns can be more easily addressed and minimized.

The USMC also relies on policy, user agreements, and training to inform participants that when utilizing the organizational or enterprise side of the device, traffic is forced through the USMC-VPN, which allows for inspection and monitoring as if working from a government system. Monitoring user activity on a government system or network is a practice, with which government employees and contractors are well accustomed and widely accept. Conversely, the personal instantiation utilizes commercial Internet or cellular service to send and receive traffic. Therefore, the personal traffic is not monitored or even seen by the organization, which in essence, preserves a user's privacy.

A key concern when implementing a BYOD program is the development of sound policy. By leveraging known security controls and lessons learned from the aforementioned case studies and applicable publications, the USMC can more effectively develop a policy that strikes the right balance between security, privacy, and convenience. As a result, Chapter IV discusses the policy development methodology, as well as considerations and recommendations as they relate to the development of USMC BYOD policy.

[221] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 7.

# IV. BYOD POLICY DEVELOPMENT METHODOLOGY AND CONSIDERATIONS

To provide a more detailed analysis of the established security controls associated with the case study subjects, an effort was made to identify every security control from the three case study user policies with possible applicability to the USMC BYOD program. These applicable case study controls were then utilized as a starting point to develop a viable BYOD user agreement for the USMC.

## A. METHODOLOGY

With regard to information assurance (IA), an adversary's primary goals can be grouped into three general categories: "unauthorized access, unauthorized modification, and denial of authorized access."[222] Adversaries attempt to leverage any number of vulnerabilities to accomplish these goals. The intent of an information security policy is to establish an organizational target for what it means for its systems and data to be secure, which in turn, leads to a set of countermeasures or controls, which when adhered to, reduce risk to a level acceptable to the organization.

The purpose of developing this proposed BYOD user agreement is twofold, 1) to mitigate some of the inherent risks associated with implementing a BYOD program on unclassified MCEN, and 2) to communicate risk to the end users with respect to their property and data. As outlined in FIPS Publication 199, the three security objectives for information and information systems are confidentiality, integrity, and availability (CIA).[223] To this end, a baseline of security controls (and associated security enhancements) applicable to BYOD have been identified from the NIST Special Publication 800-53 Revision 4 (SP-800-53), *Security and Privacy Controls for Federal*

[222] National Security Agency Information Assurance Solutions Technical Directors, *Information Assurance Technical Framework (IATF) Release 3.1* (Fort Meade, MD: IATF Manager, National Security Agency, 2002), 4–1, http://www.dtic.mil/docs/citations/ADA606355.

[223] Information Technology Laboratory National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS Publication 199) (Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2004), 2, http://csrc nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

*Information Systems and Organizations.*[224] These baseline controls were then compared and mapped to the corresponding standards listed within the user agreements collected from the TTB, the EEOC and the CPG. The compiled list of controls from the previous two steps was then narrowed to a set of policy standards relevant to the USMC's BYOD program. Finally, these controls were also compared to applicable DOD and USMC policies to create the proposed BYOD user agreement (Appendix B) to support the technological solutions being evaluated by the USMC. Factors considered for policy development, as well as the methodology, are depicted in Figure 1.

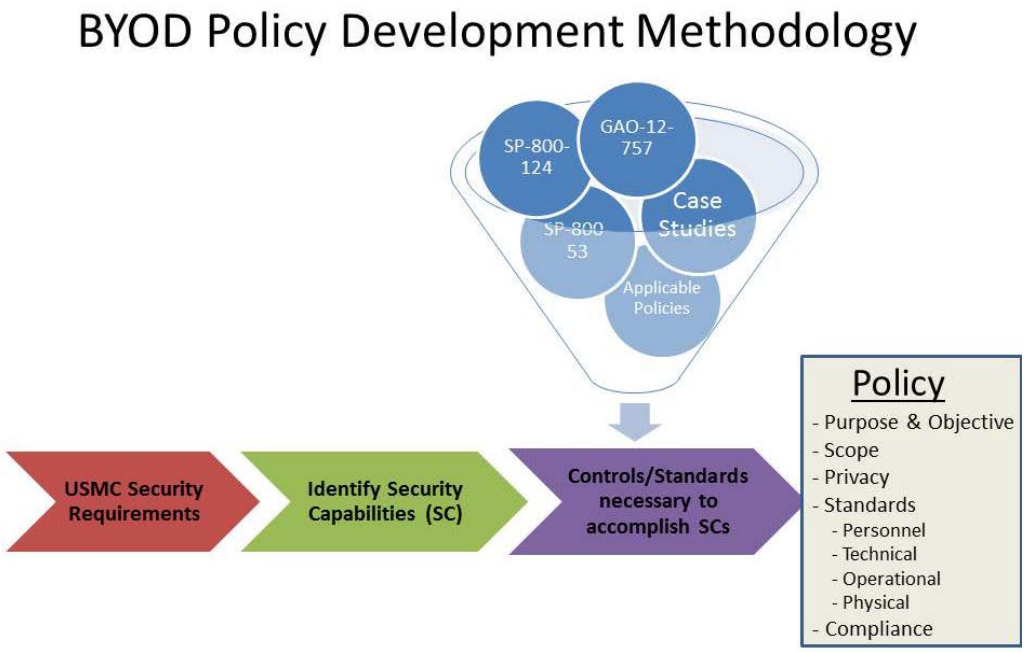


Figure 1. BYOD Policy Analysis and Development Methodology

### 1. Methodology Definitions

This section describes and defines facets of the policy development and control selection methodology depicted in Figure 1.

As discussed in the first section of Chapter II, security requirements are applied to an information system to ensure the confidentiality, integrity, and availability of the

[224] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*.

information being processed, stored, or transmitted.[225] The USMC BYOD security requirements are secure remote authentication, maintaining device OS integrity, and the protection and control of the organizational network and data.

The concept of security capability is a construct that recognizes that the protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control).[226] NIST SP-800-53 defines a security capability as "a combination of mutually reinforcing security controls (i.e., safeguards/countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and/or procedural means (i.e., procedures performed by individuals)."[227] In most cases, such protection results from the selection and implementation of a set of mutually reinforcing controls.[228] Thus, an organization can consider defining a set of security capabilities as a precursor to the security control selection process.[229] In taking this approach, a set of security capability requirements were identified based on the USMC provided security requirements, followed by identifying the necessary security controls to accomplish these requirements. For the USMC's BYOD program, the security capability requirements follow the principles of the CIA triad and align with and address the primary security requirements as delineated by the USMC. The U.S. Marine Corps Chief of the Vision and Strategy Division stated, "the organizational container has two pieces that must be protected: the VPN connector and the derived PKI credentials. The security of the encrypted data containers is also a major concern as we must ensure that if lost or compromised, the data container remains intact and the intruder cannot use the device to access the network."[230]

---

[225] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, B–23.

[226] Ibid., 21.

[227] Ibid., 20.

[228] Ibid.

[229] Ibid., 21.

[230] Anderson, May 16, 2014.

Appendix A lists the controls set forth in the case study user agreements (TTB's, EEOC's and CPG's). Each case study policy control has been mapped to the corresponding security control(s) and associated enhancement(s) listed in the NIST SP-800-53. Additionally, the three primary security requirements provided by the USMC are matched to each control as are the IA concerns that each policy control is designed to address. Many of the SP-800-53 security controls overlap and complement each other, which creates a security capability. Thus, the overlap of security controls is evident in Appendix A, as multiple SP-800-53 derived security controls often apply to any one organizational policy standard. Although not listed in Appendix A, NIST SP-800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," and GAO-12-757, "Better Implementation of Controls for Mobile Devices Should Be Encouraged," echo many of the same security control considerations.[231] SP-800-124 and GAO-12-757 controls are not listed in Appendix A because the SP-800-53 is the governing security controls document identified for this research. Listing the associated controls from the SP-800-124 and GAO-12-757 would therefore be redundant. However, it is important to be aware of the amplifying information and guidance contained within these two publications for reference in the endeavor to develop a viable BYOD user agreement.

## B. DEVELOPMENT

The review of numerous development recommendations, as well as existing DOD and DON user agreements, identified broad disparities, in both user agreement format and content. However, to best serve the Marine Corps' BYOD program, the following six sections have been recognized as common or essential components, with background being optional: purpose or overview, objectives, background, scope, standards, and compliance. The *purpose* describes why the policy is being implemented. It defines the challenge that the policy is addressing and ensures that everyone affected by the policy

[231] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Report to Congressional Committees, Managing the Security of Mobile Devices in the Enterprise*; U.S. Government Accountability Office, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*.

understands its content and applicability.[232] To establish a common understanding, it may also be necessary to define terms.[233] *Objectives* describe the expected outcome as a result of policy enforcement.[234] The researchers have chosen to combine the purpose and objectives sections to create a more coherent BYOD policy. Although not required, a *background* section is also beneficial to add historical context to a policy and to amplify the intent. A policy *scope* identifies those who might be affected by a policy or to whom the policy applies.[235] *Standards* provide organizational-level directives regarding acceptable methods or user behaviors.[236] For instance, these rules within a BYOD program might consist of how organizational data can be accessed or how organizational email can be used. The last section of a policy is *compliance*, which clearly states the possible consequences of not adhering to the standards and guidelines as listed in the user agreement.[237]

Careful considerations regarding the length of this proposed user agreement were also considered. Problems with user agreement length are twofold. First, if the document is too short, various guidelines or controls will either be addressed vaguely and ambiguously, or not addressed at all. Second, an overly long user agreement creates a situation in which employees may not read it, or they may read it and not retain the content. The TTB, the EEOC, and the CPG's BYOD user agreements range from three to six pages in length, which became our target range to provide clear and retainable information to BYOD users.

Finding the correct policy balance can also reduce some legal issues associated with BYOD by protecting both the organization and the employees. Early BYOD user

---

[232] Tom Olzak, "Security Basics—Components of Security Policies," *brighthub.com*, May 7, 2010, http://www.brighthub.com/computing/smb-security/articles/2259.aspx.

[233] Ibid.

[234] Ibid.

[235] Paul Cichonski et al., and National Institute of Standards and Technology (U.S.), *Computer Security Incident Handling Guide* (NIST Special Publication (SP) 800-61 Revision 2) (Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2012), 8, http://csrc nist. gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

[236] "What Is a Policy Statement?," accessed July 14, 2014, http://education-http://education-portal. com/academy/lesson/what-is-a-policy-statement-definition-examples-quiz.html.

[237] Olzak, "Security Basics—Components of Security Policies."

agreements were simple and vague.[238] These early agreements did not provide clear rules for behavior and "consisted of generalizations about what organizations and employees can and cannot do."[239] As a result, these BYOD agreements were, for the most part, inadequate when referenced for discovery or when employees voiced privacy concerns.[240] Lawyers subsequently became involved to help companies draft detailed agreements encompassing numerous scenarios to include legal cases for e-discovery.[241] BYOD agreements grew in length and "favored the company's right to monitor, access, review, and disclose company or other data on BYOD mobile phones and tablets."[242] Additionally, early agreements provided little consideration to an employee's expectation of privacy, which raised concerns that organizations were violating the National Labor Relations Act by placing too much control over an employee's use of the Internet, BYOD, and social media.[243] Many of these concerns are allayed based on the USMC technological solution, which creates separate personal and organizational instances, but must still be considered for policy application.

### 1. Development of Security Control Categories

To simplify the presentation of the proposed user agreement and create a coherent format that BYOD participants can easily read and logically follow, the applicable standards were parsed into four categories: personnel (administrative), technical, operational, and physical. These categories were determined after studying how various controls are described and categorized in applicable DOD guidance, the NIST SP-800-53, the Information Assurance Technical Framework (IATF), as well as the BYOD policy and legal considerations put forth by Littler Mendelson, P.C.

---

238 Tom Kaneshige, "How BYOD Puts Everyone at Legal Risk," *CIO*, November 21, 2013, http://www.cio.com/article/2380725/byod/how-byod-puts-everyone-at-legal-risk.html.

239 Ibid.

240 Ibid.

241 Ibid.

242 Ibid.

243 Ibid.

The NIST SP-800-53 security control catalog consists of 18 control families with numerous controls and enhancements listed within each family of controls.[244] The 18 control families are too specific for user agreement application. However, the SP-800-53 lists three categories in which these 18 control families can fall: management, operational, and technical.[245] Although a great starting point, identifying management as a category for policy has the possible connotation of "only applying to management." Also listed in the SP-800-53 are the three ways in which a security control can be implemented via technical, physical, and procedural means.[246] Littler Mendelson, P.C. puts forth a myriad of excellent policy considerations for the implementation of a BYOD program, but narrowly assigns the categories of technical controls and operating procedures.[247] DOD Directive (DODD) 8500.01E establishes policy and assigns responsibilities to achieve DOD IA through the integration of personnel, operations, and technology.[248] The breakdown of personnel, operations, and technology listed in DOD Directive 8500.01E provides a manageable set of categories under which each BYOD policy standard can apply. The IATF identifies the same factors as DOD Directive 8500.01E in support of IA. The IATF states, "information assurance relies on *the people*, *the operations*, and *the technology* to accomplish the mission/business and to manage the technology/information infrastructure."[249] The categories of operations and technical were common among most of the aforementioned sources. However, it was determined that the control categories of personnel, operations, and technology, as listed in both the DODD 8500.01E and IATF, was the better approach because these categories best capture the required facets of most any IA or IT related policy.

---

[244] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, F1–233.

[245] Ibid., F3.

[246] Ibid., 20.

[247] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 50–52.

[248] Department of Defense, *Information Assurance (IA)* (Department of Defense Directive (DODD) 8500.01E) (Washington, DC: Department of Defense, 2007), 1, http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf.

[249] National Security Agency Information Assurance Solutions Technical Directors, *Information Assurance Technical Framework (IATF) Release 3.1*, iii.

To this list of personnel, operations and technology, the category of physical controls (as identified in the SP-800-53) was added. Physical security or protection of a mobile device is of significant importance and worthy of a separate category because it is precisely the mobility and small form factor of these platforms that separates them from a traditionally stationary IT resource.[250] In the past, and because it is not portable, an organization did not have to worry about employees losing their desktop computer at the airport. Furthermore, because the computer stayed in a secured office or building, the possibility of an employee's desktop computer being stolen was also not a significant concern. The mobility and small size of the devices utilized within a BYOD program require additional physical protection, which will be incumbent upon the employee to perform.

As addressing privacy concerns is a major portion of this research, a separate section regarding privacy was also added. Moreover, the researchers felt it important to separate the issue of privacy because as described in the case of the CPG, numerous employees expressed concerns regarding privacy associated with organizational legal holds to support data discovery, as well as location services. Therefore, it is best to address privacy within its own section because employees who choose to participate in the Marine Corps' BYOD program are likely to have similar concerns.

In some cases, the aforementioned references clearly place individual security controls within a specific control category (e.g., personnel, operations, technical). In such cases, security controls are categorized accordingly. However, often these references do not clearly categorize many of the security controls. In those cases in which no clear indication of a control's classification exists, security controls were categorized based on where such controls best fit within the proposed user agreement or how the control will be implemented (e.g., technical, physical, or procedural).

[250] Souppaya, Scarfone, and National Institute of Standards and Technology (U.S.), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, 4.

### 2. Analysis and Recommended Controls to Support USMC Security Requirements

To satisfy the USMC security requirements, research efforts were able to narrow the list of pertinent controls because many overarching security capabilities should already be established within components of the MCEN, which is the infrastructure through which organizational data will be accessed and organizational BYOD traffic will traverse. As an example, role-based access control policies that describe which users can access which files are already established within the MCEN. The USMC BYOD program inherits these controls, and thus, it is not necessary to address them explicitly in BYOD policy. As previously discussed, Appendix A provides amplifying details regarding the case study user agreement controls and how they correlate to the USMC's primary security requirements.

Based on the primary security concerns and the technological solutions being considered, the next section describes the controls necessary to support the USMC's BYOD program and why certain controls have been selected. Many of the policy controls identified in Appendix A are similar to those identified within the draft Marine Corps Portable Electronic Device user agreement and associated policies; however, several differences have been identified and are worthy of further discussion.[251] The USMC is adopting a robust set of technological solutions to address its primary BYOD security requirements. However, the application of acceptable use controls to compliment these technological solutions will help to further address and mitigate these security concerns.

## C. PRIMARY SECURITY REQUIREMENTS

The three primary security requirements, as identified by the USMC, and how the USMC's technological approach supports these requirements are the topic of this section. User agreement and additional technical control recommendations are also discussed to support these security requirements.

---

[251] United States Marine Corps, *Draft Blocks 13-16 System Access Authorization Request (SAAR)*, Department of Defense (DD) Form 2875, provided by Robert Anderson (Chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), email message to the author, September 25, 2014.

### 1. Controls to Support Secure Remote Authentication

The technological solutions being evaluated by the USMC provide a sound process for secure remote authentication and adhere to the guiding principles listed in the SP-800-53. Since the derived credentials are resident on the personally owned device, the USMC considers the device itself as "something you have."[252] Therefore, the derived PKI credentials resident within the organizational container coupled with a required PIN ("something you know") establishes two-factor authentication while the VPN protects data-in-transit. Moreover, the USMC requires a PIN (or similar access mechanism depending on device type) to access the phone initially, followed by a username and password to access the organizational container. This being the case, the protection of access credentials becomes one of the primary user controls and is easy to address within the user agreement.

Since logical access to the organizational container uses single-factor authentication, passwords must comply with the complexity and maintenance requirements as outlined in Defense Information Systems Agency (DISA) security technical implementation guide (STIG) for application security and development.[253] This STIG provides guidance regarding password complexity, reuse, length, and periodic change requirements to name a few.[254] Adherence to this password guidance for accessing the organizational container protects organizational data resident on the device and supports secure remote authentication. If participants cannot access the container, they cannot access the VPN connector and derived credentials necessary to establish a remote connection to the MCEN.

Additional controls associated with maintaining the device OS integrity and configuration settings, as well as the encryption of the organizational container, provide layers of defense in depth to support the secure remote authentication requirement. The

---

[252] Anderson, December 30, 2014.

[253] Defense Information Systems Agency, *Application Security and Development, Security Technical Implementation Guide (STIG) Version 3 Release 9* (Ft. Meade, MD: Defense Information Systems Agency, 2014), 42–43.

[254] Ibid.

process to register and activate a device in the USMC BYOD program ensures approved device accountability while also establishing proper configuration settings. An iOS user, for example, downloads the AT&T Toggle application from the Apple store.[255] The USMC provides an enterprise activation code to the user and also sends an email with guidance to configure the personally owned device properly.[256] The settings specified in the STIG are then remotely applied to the organizational container application.[257] This basic process is the same for all device types. Technological solutions are in place to identify the device and to ensure the device falls within acceptable parameters prior to being allowed access to the MCEN.[258] Based on the USMC technological solution already in place, secure remote authentication is quite possibly the easiest security requirement to address within the user agreement.

User agreement controls identified from the case study organizations can be incorporated into the USMC BYOD policy to augment secure remote authentication. For example, a BYOD participant must log off and disconnect from the VPN when done working. Technological solutions should also be in place to enforce this requirement, such as an automatic disconnect following five minutes of inactivity. The same control should be in place for the organizational container. This control has the added benefit of protecting organizational data and networks should a user forget to log out of the organizational container or disconnect from the VPN providing unfettered access if a device is subsequently lost or stolen.

Following a set number of failed attempts to enter the correct PIN, a technological solution should be in place to block VPN access from a personally owned device. Optimally, the failed VPN access attempts should also automatically log out of and lock the organizational container until the participant is able to contact the USMC helpdesk to unlock the container and restore the capability to establish VPN connections. As an added measure of defense-in-depth, a remote wipe of the organizational container could also be

[255] Anderson, September 23, 2014.

[256] Ibid.

[257] Ibid.

[258] Ibid.

initiated. The same controls should also be put in place to protect the organizational container from unauthorized access.

Split tunneling is not a significant concern as a result of the separation provided by the Marine Corps' BYOD technological solution. Split tunneling means that a remote or VPN client may maintain a VPN tunnel with the MCEN while also directly communicating with non-MCEN systems. While working inside the organizational container, all Internet traffic traverses the MCEN VPN. However, possible vulnerabilities exist within the USMC BYOD solution regarding a non-traditional "split-tunnel" via the physical connection of a personally owned mobile device to a non-organizational system.

Synchronizing and backing up data stored on personally owned mobile devices require clear policy guidance. Directly connecting personally owned mobile devices to government IT resources is not allowed, but additional considerations must also be addressed within acceptable use policies. For instance, the BYOD participant must terminate an active VPN connection and log out of the organizational container prior to directly connecting a personally owned device to a personal computer, storage, or any other external device. The most favorable approach would be to incorporate a technological capability in which the mobile OS detects the direct connection and automatically terminates the VPN connection and prohibits access to the organizational container throughout the duration of the direct connection. This control will mitigate a myriad of possibilities associated with a non-organizational computer establishing a connection to the MCEN, the introduction of malware onto the network, and prevents the backup of organizational data to a non-organizational information system.

Furthermore, backing up organizational data to cloud-based storage services, such as iCloud and Dropbox, should be explicitly prohibited. Technical solutions, such as the blacklisting of cloud-based storage websites, should also be in place to enforce this policy. Additionally, the agreement should state that BYOD participants will not attempt to circumvent the separation between the personal and organizational side of the dual use device to include emailing government information from an official email account to a personal email account, such as Gmail or Hotmail.

The agreement should state that the USMC is not responsible for lost or stolen personally owned devices or lost personal data stored on the device. Backups of personal data resident on the personal side of the dual use device are the responsibility of the participant and should be routinely performed.

### 2. Controls to Support Device OS Integrity

Maintaining OS integrity on a personally owned device is possibly the most important security requirement for the USMC BYOD program as the ramifications of a compromised OS effect both secure remote authentication and the protection and control of organizational networks and data. Specific guidance and associated disciplinary actions regarding attempts to root or jailbreak a personally owned mobile device should be clearly stated, especially since the USMC is leaning towards the sandbox approach. Rooting or jailbreaking a mobile device compromises OS integrity, which also compromises the separation between the personal and work instantiations resident on the device. Ultimately, the VPN connector, derived PKI credentials and data resident within the organizational container would no longer be secure, which could also create a worst case security scenario, which is unauthorized access to the MCEN.

The USMC security practice of automatically encrypting the organizational container through the utilization of AES 256-bit encryption in addition to the access controls in place makes unauthorized access to organizational data and the MCEN unlikely.[259] The USMC is confident that if individuals attempt to exploit the organizational container, for example via a random access memory (RAM) dump, they still cannot glean much (if any) meaningful data from inside the container as a result of the encryption.[260] However, a rooted or jailbroken device can introduce malware capable of capturing keystrokes and screen shots, which can then be used to conduct a myriad of additional exploits.[261] According to McAfee, 2.4 million samples of new mobile malware

[259] Anderson, December 30, 2014.

[260] Ibid.

[261] Brian Donahue, "Mobile Malware Captures Keystrokes, Screengrabs," *Threatpost*, January 30, 2014, http://threatpost.com/mobile-malware-captures-keystrokes-screengrabs/103973.

emerged in 2013.[262] The presence of malware on a personally owned device increases the likelihood of unauthorized disclosure and can also establish root access. It is, therefore, imperative that participants adhere to user agreement controls that also require maintaining and applying available updates to the original mobile OS, as well as prohibit the downloading of unauthorized third-party applications.

The relevant controls listed in the case study user agreements can be leveraged to address this security requirement. For example, the user will not install unauthorized software or make any attempt to jailbreak the personally owned device. Conversely, only applications from organization-approved application stores (i.e., the DISA Mobile App Store) may be downloaded and utilized within the organizational container. A whitelisting approach to MAM is recommended within the organizational container because it would be easier to track and manage permitted applications in this environment. Whereas a blacklisting approach on the personal side of the device is recommended to protect against known threats to mobile platforms that may also pose a threat to the integrity of the organizational container. Taking a whitelisting approach on the personal side of the device will prove difficult to manage and will also place too much of a constraint on a BYOD participant's personal use.

The ability to detect a compromised mobile OS or unauthorized software also ensures BYOD participants can use the personal side of the device as they choose. Careful and routine use of a personally owned device—such as basic web browsing or opening an email attachment from a trusted source—can still result in the inadvertent download of malware. Therefore, having this technological solution in place to support user behavior is vital to allowing participants the freedom to access organizational resources when and where they need it, while not limiting the personal use of a device to the point in which participating in a BYOD program is not beneficial. However, participants must be aware that certain activities conducted on the personal side of the device can have adverse impacts on the organizational side.

[262] Kate Vinton, "Mobile Malware Is on the Rise, McAfee Report Reveals," *Forbes*, June 24, 2014, http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/.

The USMC technological solutions under evaluation have the capability to detect when a device OS has been altered; however, this detection capability is not completely effective.[263] If it is an acceptable risk to the USMC, then the technological solution to detect the rooting or jailbreaking of a device coupled with BYOD user adherence to the agreement is required to counter this risk to the greatest extent possible.

The containerization approach certainly adds a layer of defense through access control and encryption for data-at-rest; yet, technical solutions can do very little to counter social engineering and phishing attempts. Therefore, initial and annual training requirements must be in place as attackers will also seek to exploit personally owned mobile devices and the organizational data they contain through what is arguably the weakest security link, the device user.

Device OS integrity is also supported through additional user agreement controls identified from the NIST SP-800-53 and the case study organizations. Although such technological solutions check for device configuration settings, the user agreement should also stipulate that participants will not alter these settings. Furthermore, personally owned devices should be inspected by the organization following foreign travel to ensure proper configuration and to ensure no signs of physical tampering prior to resuming its use to access organizational networks and data. Certain configuration changes may also need to be considered prior to foreign travel, especially to those countries or areas deemed as high risk. This research recommends disallowing the use of personally owned devices to access enterprise resources while outside of U.S. territories and Canada. Instead, a small stock of government furnished devices can be configured and checked out before conducting official travel to moderate or high-risk countries. Recommended practices for unofficial travel are discussed in Section E, Subsection 6 regarding overtime.

[263] Fetterman, August 26, 2014.

### 3. Controls to Support the Protection and Control of Organizational Data

Technical solutions are in place to protect organizational data. The USMC organizational container (and all content) is encrypted utilizing AES 256-bit encryption. This protection of data-at-rest is important because as discussed, the VPN connector and derived PKI credentials could be utilized to gain unauthorized access to the MCEN. Furthermore, participants have the latitude to save sensitive (not classified) information within the organizational container. In addition to the credentials required to access the organizational container, and the network access controls (NAC) in place to detect a compromised device, additional layers of defense-in-depth are provided through encryption and the ability to remote wipe the organizational container.

It is important for the agreement to clarify the fact that all information stored, processed, or transmitted within the organizational container belongs to the USMC. The user agreement should stipulate that saving organizational data to cloud-based storage services is strictly prohibited, as these services cannot guarantee confidentiality, and may result in a situation in which data resides outside of organizational control. Blacklisting websites associated with such services will support this control. However, blacklisting these sites could stifle some coordination efforts with organizations outside of the USMC. Additionally, only authorized individuals are allowed to post organizational content online. This control addresses multiple concerns associated with operational security and mitigates the possible posting of sensitive information not approved for release. Attempts to circumvent or bypass these controls should also be prohibited to include emailing organizational data from an official email address to a personal email account.

To ensure the protection and control of organizational data further, guidance is required to handle the separation or transfer of employees. A process should be developed to ensure managers or human resource departments notify BYOD administrators of such personnel issues so that the organizational container can be wiped from the associated personally owned device. The user agreement should also clarify that a remote wipe of the organizational container will be initiated upon notification of a

participant's separation from the organization. Assuming an employee leaves the organization under favorable circumstances, the requirement to checkout with the IT department and BYOD administrators can be incorporated into the checkout process. This process can also be used to ensure accountability of BYOD participants and to support the transfer of military personnel to new duty stations.

Additional issues need to be considered with the transfer of military personnel. For example, it may be advisable to terminate or suspend VPN access to the MCEN at checkout, and subsequently, reactivate or reenroll the service member during check-in at the next duty station. Suspension and transfer of BYOD access would allow the participant to utilize the same credentials at the service member's next command following the successful completion of BYOD enrollment. Whereas termination may require wiping the organizational container at checkout and starting the process from scratch during check-in at the new duty station. The termination and wipe option would ensure that the new command has positive oversight of the BYOD participant. Furthermore, this practice ensures that organizational data resident on the personally owned device cannot be unnecessarily accessed or disseminated by the service member as information pertinent to the member's prior position may not be pertinent to the new position. The termination and wipe option is recommended because it can be easily administered and applied as a blanket process for transfer, separation, termination, and retirement scenarios. Alternatively, the suspension method is similar to the process for transferring individuals and security clearances in conjunction with a permanent change of duty station, which will require increased administrative overhead and coordination. Additionally, the suspension option could result in a security lapse between the gaining and losing units.

In reality, this process should probably be handled on a case-by-case basis with the service member responsible to communicate to the BYOD administrators in the event data resident within the organizational container is required for a follow-on assignment. If the service member does not communicate the requirement to retain organizational data to BYOD administrators, the protocol for addressing the transfer of a military member will default to one of the aforementioned terminate or suspend procedures.

## D. PRIVACY CONSIDERATIONS AND RECOMMENDATIONS

A common misconception associated with a BYOD program is that participation requires employees to relinquish all expectations of privacy on a personally owned device.[264] This misconception, however, is only partially correct because while employees are entitled to an expectation of privacy when using a personally owned device for dual use, the expectation is potentially lower than if they were not in the program. Even though an employee in a BYOD program may incur a lower expectation of privacy, it is nevertheless important for an organization to recognize that an employee does have certain inherent rights codified by statute, unless those rights are explicitly waived.[265] For example, both the federal Computer Fraud and Abuse Act (CFAA) and Stored Communications Act (SCA) make unauthorized access to a computer —in this case, a personal mobile device—and stored emails on a personal mobile device a criminal offense.[266] Additionally, when the organization is the U.S. government, the Fourth Amendment also applies, affirming "The right of the people…against unreasonable searches and seizures."[267]

A key concern of the USMC in implementing its BYOD program is ensuring that a participant's expectation of privacy is protected on the personal side of the device. To alleviate these concerns, The Littler Report recommends using a sandbox or virtual container approach to separate the personal side of the device from the organization side.[268] The USMC is implementing this containerized approach via its technological solution, which allows the management and protection of organizational data without needing to access personal information residing outside the organizational container. While this solution alleviates many of the USMC and participant privacy concerns, case study research revealed additional concerns common to participants that could arise when

---

[264] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 13.

[265] Ibid.

[266] Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030; Stored Communications Act (SCA), 18 U.S.C. §2701

[267] U.S. Const., amend. 4.

[268] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 51.

implementing a BYOD program. As such, in conjunction with the technological solution, it is essential that the USMC also address these concerns through policy and a carefully crafted user agreement to ensure that a user's expectation of privacy is preserved as much as possible and the terms of participation are clearly defined.

### 1. Monitoring

A stipulation in the draft USMC BYOD user agreement, which is also integrated into Appendix B, states that employees are subject to monitoring when using a personally owned device to access the organizational container.[269] The capability to monitor user activity on a government system or network is a common practice within the DOD and supports the DOD's responsibility of conducting Computer Network Defense (CND). DODI O-8530.2, Support to Computer Network Defense, states that CND is "Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks."[270] Thus, to align with broader DOD policy, the USMC is required to monitor their systems and networks. By signing a user agreement, employees provide their consent to monitoring; however, the USMC, through its technical solution, ensures monitoring is only conducted on the organizational container.

To ensure that employees are cognizant of when activities will be monitored, it is recommended that the USMC implement a notification banner. As outlined in control AC-8 of SP-800-53, a notification banner should be displayed when accessing the organizational container.[271] Additionally, this banner should inform BYOD participants of "relevant privacy and security notices consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance."[272] As an example, the banner should state:

---

[269] United States Marine Corps, *Draft Blocks 13-16 System Access Authorization Request (SAAR)*.

[270] Department of Defense, *Computer Network Defense (CND)* (Department of Defense Instruction (DODI) O-8530.2) (Washington, DC: Department of Defense, March 9, 2001), 10.

[271] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, F21–22.

[272] Ibid.

"1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

4. Use of the information system indicates consent to monitoring and recording;

5. This banner should remain visible to the user until he acknowledges the usage conditions."[273]

### 2. Legal Holds and Data Discovery

A privacy concern that exists in any BYOD program involves the organization's ability to access personal information residing on a dual use device through the process of a legal hold and data discovery. This issue is a point of contention for many employees who feel that the process is too intrusive and reduces their expectation of privacy. Regardless of opinion, legal holds when conducted in accordance with organizational regulations and policy are warranted under rule 34 of the Federal Rules of Civil Procedure (FCRP), which state, "a party must produce responsive documents and electronically stored information (ESI) that are in its possession, custody or control."[274] Therefore, it is essential that organizations draft policy and user agreements that clearly define the terms and conditions that constitute a legal hold and data discovery. Additionally, organizations should inform employees of the risks associated with a legal hold and data discovery, such as limited access to personal data and the potential loss of that data.

The technological solution currently under evaluation by the USMC helps mitigate many of the privacy concerns for both the employee and the organization that could arise from a legal hold or data discovery. The containerized approach allows for the management and protection of organizational data without needing to access personal information residing outside the organizational container. As a result, anything outside

[273] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, F21–22.

[274] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 18.

the organizational container belongs to the employee, and consequently, is not remotely accessible to the government without a court order.[275] For the USMC, this approach preserves the employee's expectation of privacy outside the organizational container. Additionally, it holds an employee responsible for any legal matters that could stem from using their personal side of the device unlawfully. In such cases, legal holds for data discovery would be handled outside of the USMC channels and require the applicable authorities to issue a court order to the employee. To eliminate the need for a court order to conduct data discovery on the organizational container, the USMC is exploring ways to mirror data that resides in the container.[276] Since the USMC cannot currently tunnel into the organizational container to validate content, mirroring would allow it to view data created by a user that resides on the organizational container and store it at remote locations under the control of the USMC.[277] Although the USMC is currently working through the specifics, as owners of the organizational container, anything mirrored would be property of the USMC. As such, legal holds for data discovery on the organizational container would be eliminated because the data would already be mirrored and available to the USMC.

### 3. Policy Compliance

BYOD policy violations determined to be intentional or a repeat violation by the same individual should be documented in employee evaluations, as well as noted within the Joint Personnel Adjudication System (JPAS) to ensure a record exists should the participant transfer and attempt the same or similar action in the future. This practice can also be utilized to determine BYOD participation sanctions and approvals, as well as identify potential insider threats. The legalities associated with this practice have not been researched, and as such, legal counsel should be obtained prior to implementing this control and the consequences of noncompliance.

---

[275] Robert Anderson (Chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), in discussion with the author, January 22, 2015.

[276] Ibid.

[277] Ibid.

## E. ADDITIONAL POLICY CONSIDERATIONS

The policy considerations discussed in the following sections do not directly apply, in all cases, to one of the previously listed primary security requirements. For example, facets of BYOD program management are discussed. However, in many cases, it is easy to identify negative security consequences if a BYOD program is not properly managed. Additional ideas are pondered to invoke more thought regarding not only the potential risk to USMC networks and data when BYOD participants do not adhere to policy, but also potential vulnerabilities within a BYOD program that an adversary might seek to exploit.

### 1. Device Maintenance

Based on the USMC technical support model, the enterprise helpdesk will provide maintenance support for the organizational container only (i.e., derived credentials, VPN connector, enterprise applications, configuration settings).[278] BYOD participants will be responsible for any problem or malfunction outside the organizational container. In such instances, participants can take the personally owned device to their mobile carrier, manufacturer, or any number of private maintenance providers.

External maintenance of a personally owned device could present a vulnerability or threat vector to the MCEN. Stuxnet displayed how malicious code can be introduced to cripple industrial control systems by forcing equipment to shut down or run outside operational parameters to cause engineering casualties.[279] How much easier would it be for a foreign intelligence entity (FIE) to implant or recruit personnel working at these types of businesses to load malicious code or software on a personally owned mobile device under the auspices of routine maintenance? This scenario could create a significant threat vector for the MCEN, especially as the number of BYOD participants grows in fleet concentration areas. Although the technological solutions in place will help to detect such tampering or the installation of unauthorized software, it is not difficult to

[278] Anderson, September 23, 2014.

[279] Brendan Galloway and Gerhard P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Survey & Tutorials*, 15, no. 2 (Second Quarter 2013): 875, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6248648&isnumber=6512259.

imagine a scenario in which highly specialized malware could be introduced with the ability to bypass these technological controls. The practice of identifying approved maintenance providers with vetted technicians is not practical. Therefore, policy should state that BYOD participants must have their personally owned devices inspected for tampering following any maintenance performed by a third party.

Policy should clarify that the USMC is not responsible for malfunctions, defects, or damage to a personally owned mobile device; therefore, the participant should not expect reimbursement for maintenance performed on the personal side of the device.

### 2. Device Inventory

The use of government furnished mobile devices within the MCEN is easier to administer and track, as device inventory is centrally managed and the organization controls the issuance of these devices. However, within a BYOD environment, employees have the option of purchasing new devices at any time based on personal preference. This situation will challenge an administrator's ability to track and correlate a particular BYOD user to a specific device. Therefore, a control should be established to ensure participants first inform BYOD administrators so that appropriate actions, such as the removal of the organizational container, data, the VPN connector, and derived credentials can be accomplished prior to trading in the current device or transitioning the device to another member of the household, for example. The BYOD participant should subsequently register the new device by submitting an updated system access authorization request (SAAR), which will then allow for the installation of required software and credentials, as well as ensure the proper configuration of the new device. Without such a control, administrators will quickly lose track of personally owned mobile devices utilized within the BYOD program. Furthermore, with the VPN connector and derived credentials still present on the device, the possibility, however unlikely, exists for unauthorized access to the MCEN. Remote wiping of the organizational container will help mitigate this situation; however, if the employee trades in the mobile device just prior to a long weekend, a potential adversary will have several days to exploit the device prior to an administrator initiating the remote wipe. Encryption of the organizational

container minimizes this risk, but adherence to the aforementioned control requiring the participant to inform BYOD administrators first prior to trading or transferring ownership of a device will further alleviate this risk.

The importance of maintaining an accurate inventory of personally owned devices used to access the MCEN is also highlighted in an Inspector General's (IG) report regarding the U.S. Army's management of commercial mobile devices (CMD). The IG report identifies numerous cybersecurity related vulnerabilities due to a lack of CMD accountability.[280] These vulnerabilities stem from the fact that the Army CIO was unaware of more than 14,000 CMDs used throughout the Army.[281] As these CMDs were not accurately tracked, the CMDs were not configured to protect stored information.[282] A myriad of additional concerns were also identified to include no capability to wipe devices remotely, no ability to control CMDs used as removable media, no user training or signed user agreements, and no clear policy for CMDs purchased under pilot and non-pilot programs.[283] These shortfalls left Army networks more susceptible to attacks, as well as sensitive data leaks.[284]

### 3. Approved Products List

"The Marine Corps Commercial Mobile Device Strategy for BYOD relies heavily on separation technology within the end node terminal device to support multiple domains."[285] Therefore, only personally owned mobile devices with the capability to support multiple domains will be considered for inclusion on the authorized list of devices allowed to access the MCEN remotely.[286] The USMC is working to establish a

---

[280] Inspector General United States Department of Defense, *Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices* (Report No. DODIG-2013-060) (Washington, DC: Department of Defense Office of Inspector General, 2013), http://www.dodig.mil/pubs/documents/DODIG-2013-060.pdf.

[281] Ibid.

[282] Ibid.

[283] Ibid.

[284] Ibid.

[285] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 10.

[286] Ibid., 11.

BYOD program that will allow for the inclusion of most common device types. This program equates to a large quantity and variety of devices that will be allowed to operate within the MCEN. This being the case, it may be advisable to incorporate personally owned mobile devices in phases. This gradual approach will help ensure the smooth assimilation of mobile devices onto operational networks while easing the initial registration and administrative efforts. For example, the first two phases can work through the integration of devices utilizing Apple iOS and Android mobile operating systems, as these comprise the majority of personally owned devices within the U.S. market.[287] Following the success of the first two phases, personally owned Blackberry and Microsoft devices (if Microsoft devices are approved) can then be added.

User demand may also be a factor to consider. The EEOC only allows for the use of Android, iOS, and Blackberry devices within its BYOD program, primarily because EEOC employees have not communicated a demand for any additional or alternate device types.[288] Furthermore, the EEOC only allows Apple iOS iPad devices to establish VPN connections to organizational data centers, which minimizes configuration management requirements. Organizations can establish a small internal approved products list (APL) based on DISA's APL or allow any and all device types included in the DISA APL.[289] Establishing a minimalistic APL eases the administrative overhead and helps scope enterprise service helpdesk support requirements, such as establishing or checking configuration settings on disparate devices. Whereas a broader APL creates better flexibility for the BYOD participant, and opens up a wide range of personally owned device selection options. Obvious pros and cons exist regarding both approaches, which must be considered to ensure the proper balance of user flexibility and associated risk with administrative overhead. The underlying BYOD technological solution will also

[287] Jess Scanlon, "What Is the U.S.'s Most Popular Smartphone?," *Wall Street Tech Cheat Sheet*, June 4, 2014, http://wallstcheatsheet.com/technology/what-is-the-u-s-s-most-popular-smartphone html/?a=view all.

[288] Hancher, July 7, 2014.

[289] "The UC Approved Products List: Multifunction Mobile Device," September 23, 2014, https://aplits.disa.mil/processAPList.action.

play a significant role in determining the right approach when identifying what devices will be allowed to participate.

Limiting the number of personally owned mobile devices an individual can register and use within the BYOD program should also be considered. As an example, each participant could be limited to only one device authorized for remote access (i.e., one smartphone or one tablet). Limiting device types and number of devices allowed for each individual BYOD participant will reduce some of the challenges associated with forensic analysis and discovery, as well as remote wiping procedures. The number of devices that a command allows a participant to utilize should depend on the individual's level of responsibility, as allowing one individual to utilize multiple personally owned devices to access the MCEN will increase the operating costs associated with paying for more client access licenses.

#### 4. Separation of Duties

Compared to the organizations researched, the USMC's BYOD program is unique in its technological approach, as well as the individuals it employs. Private sector and non-DOD government agencies consist of civilian or government civilian employees and contractors, whereas the USMC also employs active duty and reserve component Marines. BYOD policy criteria could limit participation only to full-time civilians, contractors, and Marines who will be assigned and continuously supporting a USMC command for six months or more. In the case of part-time employees or reserve component Marines involved in a typical one weekend per month and two weeks per year drill schedule, the basic ability to sync email, calendars, and contacts may be sufficient.

Another possible scenario involves a government civilian or contractor who works for a Marine Corps command, and is also a reserve component Marine. This situation may become problematic and have legal implications if access to the MCEN based on roles and responsibilities are not clearly separated. A potential solution in this case may be the creation of two organizational containers on a personally owned device; however, it is unknown at this time whether the USMC BYOD technological solutions under evaluation can support this option. The current USMC solution to this situation is

to issue two separate common access cards (CAC).[290] Both accounts within Active Directory (AD) have their own user profiles and associated email addresses. The exchange server does have the capability to associate one user profile with two separate email addresses if in the same domain (i.e., usmc.mil).[291] However, this issue also brings into question PKI credentials and how they are mapped to the user profiles. Separate from the technological solution used to address this problem, and whether the Marine Corps decides to limit BYOD participation to full or part-time employees, this issue—as it relates to BYOD—can be at least partially addressed through policy stating that an individual is not to access the MCEN for purposes outside the scope of assigned duties. This policy control will establish the general terms for remote access based on a user's role, as well as create a foundation for disciplinary action should investigations reveal that an individual abused permissions not associated with an assigned responsibility.

### 5. Labor Standards and Government Furloughs

In general, active duty and reserve component Marines in an active status fall under the *exempt* status with respect to the Fair Labor Standards Act (FLSA). However, government agencies must be able to adjust and adapt to broader legislative issues, such as the furlough of government civilians because of sequestration. In the event of a furlough—such as those caused by a lapse of annual appropriations—non-essential government civilians are legally prohibited from conducting any government business even on a voluntary basis.[292]

To provide a clarification of terms, a government civilian employee identified as exempt in block 35 of the Standard Form 50 (SF50) is not covered by the minimum wage and overtime laws present in the FLSA.[293] "Generally, exempt employees, because of

---

[290] Robert Anderson (Chief of the Vision and Strategy Division, Headquarters U.S. Marine Corps, Command, Control, Communications and Computers (C4), Washington, DC), email message to the author, October 17, 2014.

[291] Ibid.

[292] "Guidance for Shutdown Furloughs," 3–4, October 11, 2013, http://www.opm.gov/policy-data-oversight/pay-leave/furlough-guidance/guidance-for-shutdown-furloughs.pdf.

[293] "Standard Form 50, Revision 7/91, FPM Supp. 296-33, Subch. 4," July 1991, http://www.gsa.gov/portal/forms/download/115474.

their positional duties, responsibilities and level of decision making authority, are exempt from the overtime provisions of the FLSA, while nonexempt employees are eligible for overtime and are typically paid on an hourly basis."[294] However, the fact the employee is recognized as exempt does not broadly recognize an individual as *mission essential*, and consequently, allowed to work during a furlough. This situation creates an added challenge to ensure that both exempt and nonexempt government civilians are not conducting work for which pay is not authorized.

Moreover, the Antideficiency Act does not allow for the authorization of any expenditure or obligation before an appropriation is made, unless authorized by law, thus solidifying the fact that unless identified as mission essential, government civilian employees cannot be paid for work conducted during a furlough.[295] In this same vein, contractors are not allowed to charge hours against a contract for which appropriations have lapsed.

To address these nonexempt and furlough issues, policy should be developed to clearly state when a device can (or cannot) be used for work-related activities. However, covering furlough scenario guidance will add unnecessary length and confusion to a BYOD policy and user agreement. Instead of attempting to clarify furlough-operating procedures within the standard BYOD user agreement, it is recommended that furlough guidance be developed separately from the BYOD user agreement or added to existing furlough policy to address this infrequent occurrence.

During a furlough, government employees participating in a BYOD program will likely attempt to keep up with work requirements to avoid the inevitable mountain of backlog emails and tasks they will confront upon furlough termination. To ensure adherence to applicable statutes, network administrators should have the ability to restrict VPN connections to the MCEN for those non-essential employees during a furlough and

---

[294] Matthew D. Keiser, Kristen E. Ittig, and Emma Broomfield, "Guidance for Federal Government Contractors: What to Do with Your Employees during the Shutdown," *Association of Corporate Counsel*, October 10, 2013, http://www.lexology.com/library/detail.aspx?g=9464bb86-bcca-4e31-a013-ce4ec7448c7e.

[295] "Antideficiency Act Background," accessed October 12, 2013, http://www.gao.gov/legal/lawresources/antideficiencybackground.html.

prevent unapproved overtime. Such a technological capability can also be extended beyond BYOD to prevent furloughed employees from performing unauthorized work from both in-office IT resources and via home systems used for telework.

The TTB is the only case study subject with a BYOD solution on par with the USMC technological solutions being evaluated. For its part during the early fiscal year 2014 sequestration and associated furlough of government civilians and contractors, the TTB suspended Active Directory (AD) accounts for all furloughed employees by script.[296] The TTB uses RSA devices for remote access, which provides for two-factor authentication. Since RSA first checks AD before authenticating, suspending the AD accounts blocked both remote access and internal access.[297] Thus, furloughed employees could not access the organizational network nor have access to any information that traverses the TTB network, such as email. A similar solution via the derived credentials associated with the USMC BYOD program may be possible to prevent furloughed employees from establishing a VPN connection. The better solution would include the capability simply to lock the organizational container on devices owned by furloughed employees.

### 6. Overtime

An additional concern is overtime or work performed not during normal working hours. The FLSA provides guidance regarding overtime pay for employees and states, "a nonexempt employee must also be compensated for all work performed outside of normal work patterns and paid overtime wages for hours worked in excess of 40 hours per administrative work week."[298] In other words, the employee must be paid for work performed and if a way exists for the employer to know that work was performed.

---

[296] Robert Hughes (Chief Information Officer, Alcohol and Tobacco Tax and Trade Bureau (TTB), Washington, DC), email message to the author, October 6, 2014.

[297] Ibid.

[298] "Pay & Leave Pay Administration Fact Sheet: Overtime Pay, Title 5," accessed 14 September 2014, http://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/overtime-pay-title-5/.

Furthermore, the employee must still be paid even if not clearly authorized or directed to perform the work in advance.[299]

To address this issue, one option is to employ technical controls to restrict access to organizational data centers and email outside of normal working hours for nonexempt personnel (i.e., time-of-day restrictions). However, this solution may negate the benefit of establishing a BYOD program in the first place. Another option is to adopt a policy that states nonexempt employees must have a supervisor's written permission prior to conducting work—to include reading and responding to emails—outside of normal working hours. This solution also counters the intent and flexibility associated with a BYOD program. Additionally, it is impossible to predict the timing of world events and emergencies, which makes this solution fairly impractical within most government organizations.

The USMC does possess a technological solution that can track how much an individual is logged into the organizational container.[300] This being the case, policy can be put in place that requires nonexempt employees to not only record all time worked, but also time worked while off site and utilizing a personally owned mobile device outside of normal working hours. In the event a nonexempt employee reports overtime or a large amount of time spent outside of normal working hours, the employee's claim can be verified against the aforementioned USMC organizational container logs. This solution does add another layer of bureaucracy to the payroll and time-keeping process. Therefore, it will have to be balanced against current practices to ensure the benefits associated with a BYOD program outweigh any increased administrative tasks.

The simplest approach to the overtime issue is to state in the user agreement that overtime compensation associated with the use of a personally owned mobile device is not authorized without prior approval. In 2014, the United States Attorney's Office

[299] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 35.

[300] Anderson, September 23, 2014.

(USAO) under the Department of Justice finalized its BYOD policies and procedures.[301] The USAO policy states, "Overtime compensation is not available simply because a BYOD (or GFE) device is used after hours. Rather, the usual rules apply for formally requesting and authorizing any overtime compensation."[302] A similar stipulation regarding overtime pay is recommended within the USMC BYOD user agreement described in Appendix B.

The possibility exists that most nonexempt employees rarely have the need to access email or conduct work outside of normal work patterns. If this is in fact the case, then overtime and the amount of work conducted outside of normal working patterns because of BYOD, may not be a major concern. However, this consideration is worthy of discussion because of the potential for wide use and even abuse (by both managers and subordinates) as a result of the inherent flexibility that BYOD introduces. A well-trained BYOD workforce backed up with periodic reminders and clear supporting policy can mitigate the majority of these concerns. With policy clearly defined, disciplinary action can be taken if an employee does not comply.

A well-trained BYOD workforce includes those in supervisory positions. In the event individuals in a leadership position send an email to nonexempt employees outside of normal working hours, individuals should include a disclaimer or guidance in the opening or subject of the email to protect themselves, as well as the nonexempt employee with whom they are communicating. Managers could begin emails sent to nonexempt employees by stating whether the email should be addressed immediately or should be reviewed and responded to during normal working hours.[303] Variants of the aforementioned technological and policy solutions can also be applied to teleworkers to monitor and control access to the MCEN from home offices.

---

[301] United States Attorneys' Office, *United States Attorneys' Office Policies and Procedures: Bring Your Own Device (BYOD) Program*, Telecommunications & Technology Development (TTD) Staff Office of the Chief Information Officer (OCIO) (no. 3-16-200-017) (Washington, DC: Department of Justice, 2014).

[302] Ibid., 5.

[303] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance*, 37.

Mobile devices certainly make it easy to check and respond to work email during the evening or weekend, which blurs the line between work and personal life, and could be counted as hours worked. According to a 2011 study by IDC and Unisys, nearly 50 percent of individuals surveyed reported using personal devices to conduct work while on vacation.[304] To counter this issue while ensuring adherence to the FLSA, BYOD or network administrators could be added to the routing chain for leave requests submitted by nonexempt employees. By doing so, administrators can utilize technological solutions to disallow BYOD access to the organizational container while a nonexempt employee is on leave. The same applies to an unpaid leave of absence. This requirement can also be broadened to exempt employees prior to foreign travel whether for business or pleasure. In the event it is absolutely necessary to contact a nonexempt employee while on paid or unpaid leave, voice communications may still be possible, which eliminates a degree of the "fire and forget" mentality often associated with an email.

With the exception of medical emergencies, policy should also require that an employee set various out-of-office notifications on organizational email accounts and voicemail greetings to ensure awareness of the employee's out-of-office status while also providing an alternate point of contact should immediate action be required. These ideas are certainly not new, as many employees routinely make use of these practices.

As it relates to BYOD, the work performed outside of normal working hours, as well as the aforementioned government furlough scenario, leads to the additional question of what constitutes mission critical or essential personnel. As defined in the Marine Corps Commercial Mobile Device Strategy, privileged users are individuals who the Command identifies as being mission critical or mission essential, and are provided mobile government furnished equipment (GFE) or a reimbursement for using their commercial mobile device to gain access to their personal organizational data.[305]

---

[304] Frank Gens, Danielle Levitas, and Rebecca Segal, "2011 Consumerization of IT Study: Closing the "Consumerization Gap," July 2011, quoted in Garry G. Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, The Littler Report (New York, NY: Littler Mendelson, P.C., 2012), 5.

[305] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 3.

Unless an individual falls into the FLSA exempt status, coupled with being identified as essential personnel—for example, crisis action team member or in a key leadership position—there should be no expectation of being able to readily contact that individual outside of normal working hours. Personnel engaged in an "on watch" role, such as staff duty officer (SDO) are not included as exempt in this context because a government furnished duty phone is typically provided and passed between watch standers during turnover to ensure the phone number associated with such positions remains constant. Personnel in watch related roles are always expected to be contactable while in that position; however, following turnover of this responsibility, that status could fall back to nonexempt or at least to non-essential.

### 7. BYOD Participation

Although the Marine Corps' BYOD program is voluntary, another issue to consider is whether every employee should be allowed to participate at the same level of remote access. Historically, only privileged users have been allowed remote access to the MCEN via mobile devices; however, the DOD is shifting to an environment in which remote access is no longer limited to only privileged users.[306] Although it may be more technologically and administratively cumbersome to establish disparate remote access tiers based on a user's roles and responsibilities, applying the principle of least privilege for BYOD can reduce the potential attack surface associated with mobile devices.

Senior leaders (i.e., Flag or General officers and Senior Executive Service (SES) civilians) may not be eligible for BYOD due to the inherently sensitive nature and scope of responsibilities. In such cases, government furnished equipment may be the better option.

The USMC will also have to decide whether contractors, foreign nationals, or part-time employees are to be allowed to participate. Risks may be further reduced by limiting remote access to enterprise resources based on the level of responsibility and need for access, or for a particular pay grade range. For example, foreign nationals,

[306] Command, Control, Communications, and Computers Department (C4), *Marine Corps Commercial Mobile Device Strategy*, 3.

contractors, pay grades of E–1 through E–5, and GS–1 through GS–10, may not require access to organizational data centers, in which case, an alternate solution may be to limit BYOD capabilities to synchronizing email, contacts, and calendars only. This potential solution incorporates factors of access control and principles of least privilege, which can be enforced via technical controls.

### 8. Inappropriate Behavior Creating a Hostile Work Environment

BYOD participants may feel that personal use of their dual-use device while in the workplace is not subject to the same acceptable use policies as if using a government furnished device or IT resource. Even with a clear policy in place, managers will likely have to deal with a myriad of employee related BYOD challenges associated with the personal use of these dual-use devices. Examples range from the potential for the reduced productivity associated with personal text messaging, use of social media, cyber-protesting, and other miscellaneous web-based activity to illegal or criminal activities, such as child pornography, fraud, and copyright abuses. Furthermore, BYOD participants may feel that because they are using the personal side of their dual-use device, USMC equal employment opportunity (EEO) policies do not apply. For instance, employees using their personally owned device in the work place may interpret the fact that owning the device entitles them to watch vulgar, or otherwise offensive, videos with other colleagues.[307] These same individuals may also believe that by using commercial Internet service providers (ISP) via the personal side of the device somehow insulates them from USMC user policy.[308] This line of thought can also lead to a hostile work environment if an employee—whether through their personal computer or personally owned mobile device—posts defamatory comments regarding the organization, peers, or managers online. Policy should seek to ensure that employees fully understand the consequences of misusing both organizational and personally owned IT resources that could result in a hostile work environment or create a negative perception of the USMC and the personnel it employs.

---

[307] Mathiason et al., *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, 31.

[308] Ibid.

### 9. Devices in the Workspace

An additional consideration is to narrow the meaning of BYOD to limit device use in the physical workspace and instead focus on the flexibility that BYOD provides for participants while outside the office. This practice would disallow personal mobile devices in the work place and mitigate possible security issues associated with the use of mobile device microphones and cameras, as well as reduce the potential for employee distraction. Barring a clear mission requirement and designated approving authority (DAA) and cognizant security authority (CSA) approval, mobile devices are not allowed in spaces where classified material is processed and discussed.[309] Establishing similar guidelines within unclassified spaces where OPSEC and controlled unclassified information (CUI) are routinely discussed, will also serve to mitigate risk. Moreover, if an employee is working from a physical office, personally owned mobile devices are likely not necessary as IT resources and telephony are already provided by the organization. Employees should routinely back up organizational data resident within the organizational container of the personally owned device to the MCEN so that work can be accessed and continued from the office. This practice also ensures work conducted within the organizational container is backed up in the event a device is lost or stolen. Employees can then leave personal devices in lock boxes and to cover missed calls to the personal device, BYOD participants should incorporate a voicemail greeting that provides the office phone number where they can be reached during working hours.

### 10. BYOD Participant Training

The creation of a detailed training plan with regard to BYOD is beyond the scope of this research. However, training users and managers is undoubtedly a significant aspect to any information and IT security program. Organizations should, therefore, incorporate aspects of BYOD use into annual security awareness training requirements, as well as establish an initial training program that BYOD participants must complete

[309] Department of Defense, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)* (Department of Defense Directive (DODD) 8100.02) (Washington, DC: Department of Defense, 2007), 4, http://www.dtic mil/whs/directives/corres/ pdf/810002p.pdf.

prior to or within a specified timeframe (i.e., within two months) of becoming a BYOD participant. A well-trained workforce provides another layer of defense-in-depth to protect organizations. Employees should know how, when, and who to contact in the event of an incident or suspicious activity, such as unauthorized access, suspicious behavior or email content, a lost or stolen device, spillage of classified information, as well as best practices for physically protecting a mobile device.[310] Physical protection and control of the device is the responsibility of the participant. The proposed user agreement (Appendix B) includes several physical controls to remind BYOD participants of their responsibility to protect personally owned devices, while also providing procedures to safeguard personally owned devices.

In conjunction with annual training requirements, BYOD participants should read and sign a new BYOD user agreement, which can also serve as an annual audit of participant devices. Training should also address facets of social media use to include operational security concerns and the possibility for unauthorized disclosure, as well as posts that could create a hostile work environment or EEO violations. Simply using the personal side of a mobile device to post online content does not absolve the BYOD participant from adhering to USMC policies.

### 11. Participation Incentives

Although a detailed cost analysis and viable BYOD incentive program is outside the scope of this research, some monetary incentive is recommended to promote BYOD participation and offset a portion of the participant's monthly mobile costs. For example, the USAO sets a "flat fee" BYOD reimbursement cap "(e.g., $20/month in FY2014) for each month the employee uses the BYOD device to access the USAO network."[311]

It can be reasonably assumed that there will be three categories of employees as it relates to BYOD within the USMC. The first group will readily accept and participate in the program, even if it will incur additional monthly costs to the participant. The second

[310] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, F39.

[311] United States Attorneys' Office, *United States Attorneys' Office Policies and Procedures: Bring Your Own Device (BYOD) Program*.

group will consist of those employees who will not participate in the BYOD program regardless of how much the program is incentivized. The last group is comprised of those employees prone to sit on the fence and scrutinize the BYOD program. A reimbursement model similar to the USAO's program should be considered within the USMC BYOD program to help increase the participation of those individuals identified within this third group. When participation incentives are determined, the amounts, as well as those who qualify, should be specified in the user policy and agreement.

## F. SUMMARY

This chapter described a myriad of recommendations and additional considerations regarding the implementation of the Marine Corps' BYOD program. This list of recommendations and considerations should not be viewed as all inclusive, but does provide insight to the challenges that a BYOD policy must attempt to address. In fact, several of the considerations addressed in this chapter are not included in the proposed user agreement (Appendix B) because they are not necessarily a concern for the BYOD participant, but are important to consider in the formulation of the agreement. However, the considerations were researched and discussed so that in the event one or more of these considerations becomes a problem in the future, this research can be utilized as a frame of reference or starting point to make necessary policy adjustments. Moreover, several of these BYOD considerations, such as the furlough scenario, can also be addressed separately in what might be regarded as a "contingency policy" to avoid adding unnecessary length or confusion to the standard BYOD policy. Based on this research, the identified controls listed in the proposed user agreement, in conjunction with the technical controls inherent with the container solutions under evaluation, can make BYOD a reality within the USMC.

Usability, cost, and security are often at odds with each other in an enterprise environment. It is up to the USMC to decide whether the residual risks introduced by their BYOD solution are acceptable or are balanced acceptably by the benefits of BYOD.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSIONS, LIMITATIONS AND FUTURE WORK

## A. CONCLUSIONS

In conclusion, this thesis examined the importance of policy as it relates to BYOD programs, and the factors necessary for developing a BYOD user policy and agreement for the USMC. Furthermore, research was conducted on the applicable security controls, technological solutions, acceptable use policies, and user privacy considerations that accompany a BYOD program. Thorough examination of the aforementioned has resulted in a BYOD user agreement tailored to the USMC's technological solution, as shown in Appendix B. Although the user agreement exceeded the goal of three to six pages in length, the proposed user agreement answers the primary thesis question in the affirmative: it is possible to develop a BYOD user agreement that minimizes risk for all parties while also allowing for the intended flexibility. If formatted in a similar fashion as the user policies researched, the proposed user agreement is seven pages long. As is discussed below in Limitations, once a SAAR is finalized, redundant controls can be removed, which would shorten the proposed BYOD user agreement.

## B. LIMITATIONS

The researchers recognize the following limitations to their research.

- Although the general technical approach for implementing a BYOD program via an organizational container has been identified, the final vendor solution will not be determined until after completion of the pilot program. As a result, if the USMC decides to change its technical solution for BYOD, it will require minor modifications to the proposed user agreement, depending on which vendor solution is selected. The first phase of the pilot program is anticipated to be complete in May 2015, which is several months after this research has been completed; consequently, findings and lessons learned from this first phase are not available and cannot be incorporated into this research.
- The researchers were unable to conduct research on every organization that has successfully implemented a BYOD program. As such, the comparison of the three applicable case studies, as well as the lessons learned and best practices derived from research, represent a limited sample size. Notwithstanding, the three applicable case studies did provide

sufficient insight into the differing methods by which an organization can and have implemented a BYOD program.

- The USMC recently distributed a BYOD survey to gauge employee interest and opinions regarding BYOD implementation. Survey results were not collected or available for analysis during the period of this research; however, these survey results will prove valuable in the development of a BYOD incentive program.
- At the time of this research, the USMC was in the process of transitioning from the current DD Form 2875 SAAR to an updated version. As a result, some of the security controls listed in the proposed BYOD user agreement may be redundant to the security controls present in the standard user agreement for government IT resources. The proposed BYOD user agreement includes all controls that this research identified as necessary to mitigate risk to the greatest extent possible based on the USMC's technological approach. Once the USMC finalizes the new SAAR, controls identified as redundant within the BYOD user agreement can be removed to make the proposed agreement more succinct.
- The researchers recognize that although a considerable amount of research went into crafting the proposed user agreement, they are not qualified to make legal decisions on behalf of the USMC. Therefore, the proposed user agreement will require legal review prior to acceptance.

## C. TOPICS FOR FUTURE RESEARCH

The following items have been identified as potential topics for follow-on research.

### 1. Virtual Mobile Infrastructure

During the course of this research, Virtual Mobile Infrastructure (VMI) was identified as a favorable solution for BYOD implementation. VMI provides an alternate technological solution by creating an environment similar to that established by the TTB (as described in Chapter II). Additionally, VMI ensures that all organizational information remains within organizational data centers vice resident on the mobile device. Furthermore, based on limited research associated with this thesis, VMI may provide a more secure and easier to manage BYOD program. However, the VMI solution is estimated to cost over $80 per user annually, whereas client access licenses for organizational containers will cost around $40 per user annually.[312] Acknowledging that

[312] Anderson, September 23, 2014.

reducing costs is one of the primary considerations prior to implementing a BYOD program, the VMI price point is currently too high and the return on investment does not justify adopting VMI at this time. Should this solution become more cost effective, and subsequently, become adopted by the USMC or broader DOD to support BYOD, further research will be required to evaluate the necessary security controls to support this technology.

### 2. BYOD Incentive Program

An underlying objective in implementing a BYOD program is to enhance employee flexibility and productivity, while also realizing cost savings to the organization. Pending the outcome of the USMC pilot program, and as BYOD becomes more prevalent within the DOD, a study to determine the feasibility of BYOD incentive programs for both the USMC and the DOD is a topic for future research. Incentive programs, such as reimbursement, split-billing, or stipends, could potentially promote employee participation to allow for an organization to more effectively capitalize on the underlying objectives that a BYOD program offers. Topics worth examining are the following.

- If an incentive program is implemented, which approach would ensure that cost savings for the organization are realized, while at the same time, making BYOD an attractive solution for potential participants?
- Based on amount reimbursable, how will it be paid to participants (i.e., stipend, reimbursement, split-billing)?
- Who will be reimbursed (e.g., all participants to include contractors and foreign nationals, or limited to individuals identified as essential personnel, etc.)?
- If a reimbursement program is feasible, a study should address policy formulation, specifically outlining the processes and procedures involved with requesting reimbursement.

### 3. Expanding Scope to Bring Your Own Computer

The DOD Mobile Device Strategy recognizes the potential advantages that mobile devices provide to the workforce and their capability to "advance the operational effectiveness of the Department of Defense."[313] Assuming the success of the USMC

[313] Department of Defense, *DOD Mobile Device Strategy, Department of Defense Memorandum*, i.

BYOD program, and subsequent incorporation of personally-owned devices on DOD networks, a topic for future research would be the expansion of the BYOD concept to include personally-owned computers. Similar to mobile devices, many employees prefer their own laptops vice the standard client hardware furnished by parent organizations. Leveraging an employee's personal hardware has the potential to produce additional cost savings for the DOD, as well as alleviate DOD lifecycle costs and the periodic purchase of new client systems.

### 4. Government Furnished Wireless Access Points

The demand for wireless access points (AP)'s on government and military installations is increasing. For a user to capitalize on the flexibility that a personally-owned mobile device provides, it is expected that users will want to establish connections to these wireless AP's. Assuming wireless AP's become available within USMC installations, further research will be required to examine how the USMC will monitor personal traffic traversing the USMC enterprise wireless network and USMC-provided guest networks.

# APPENDIX A. COMPARATIVE ANALYSIS OF CASE STUDY ORGANIZATION SECURITY CONTROLS

In accordance with the research and policy development methodology described in Chapter IV, the tables in this appendix provide a complete list of the user agreement controls implemented by the three case study organizations (the TTB, the EEOC and the CPG). The case study controls are utilized to create a baseline for comparison between the organizations researched and to identify those security controls necessary to address the USMC's BYOD security requirements.

The first column of each table, titled "security objective/concern addressed," identifies the overarching IA security objective or concern that each associated control is intended to address. The details listed in this column centers on the practice of IA and the associated objectives of CIA; however, research attempts to also identify a more specific information assurance and security objective vice simply listing one of the CIA triad components. For example, the security capability to enforce the use of a password or PIN to protect a personally owned device supports the principles of confidentiality and integrity for data resident on the device. Access control and authentication are also listed to describe the "security objective/concern addressed" in more detail beyond just confidentiality and integrity. Many, if not most, of the controls involve aspects of all three CIA triad components; however, research has attempted to focus on the most prevalent security objective that each control is intended to address.

The second column of each table identifies the USMC security requirement that each case study policy control supports. The three primary security requirements as identified by the USMC are secure remote authentication, device OS integrity, and the control and protection of organizational data and networks. A particular case study security capability may address only one of these security requirements, but in some cases, two or all three of the security requirements are addressed to the same level of importance. For example, the case study security capability that requires users to log off and disconnect from the VPN when done working, addresses both the secure remote authentication and protection of organizational data, as well as network requirements.

Although this control could also have implications for OS integrity, it is not the most prevalent concern associated with this control, and thus, is not listed. Similar to the first column, and where possible, attempts have been made to identify the primary security requirement(s) that each policy control supports.

The third column of each table, titled "case study security capabilities/controls," identifies a specific security control listed within each of the case study user agreements. These security controls may be specific to only one of the case study organizations or common to multiple case study organizations. Efforts also combined those case study user agreement controls with a common intent. For example, the EEOC's BYOD user agreement states that email will be wiped following 25 failed password attempts, whereas the CPG will initiate a remote wipe following 10 unsuccessful attempts to enter the correct PIN. These controls have been combined in the tables to read "device wipe following set number of failed password or PIN attempts." The fourth column of each table, titled "case study organization," identifies those studied organizations that apply the associated control.

The fifth column of each table, titled "SP-800-53 controls," identifies those controls from the NIST SP-800-53 publication that relate to each of the case study security capabilities and controls listed in column three. Many of the SP-800-53 controls provide a degree of overlap and redundancy to achieve a particular security capability. The NIST SP-800-53 states, "the concept of security capability is a construct that recognizes that the protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls."[314] With the understanding that a security capability rarely relies on just one SP-800-53 control, multiple controls are required and identified to meet each of the case study organization's security capabilities. The presence of an "E" in the "SP-800-53 controls" column

[314] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, 21.

identifies the security control enhancement associated with a particular SP-800-53 control category.

A line-by-line review was performed on all 18 SP-800-53 control families, and associated security controls and enhancements to identify the NIST controls that mapped to the technologies or controls identified within the three case studies, whether partially or fully. The mapped SP-800-53 controls were then compared to the NIST SP-800-124 and GAO-12-757 to mitigate the possibility of overlooking applicable controls. The aforementioned analysis methodology, as well as the overlap and redundancy inherent with most SP-800-53 controls, helps minimize the potential that a required BYOD user policy control was not identified.

Finally, the case study security capabilities and controls have been separated into four tables by the categories of personnel (Table 2), technical (Table 3), operating (Table 4), and physical (Table 5) as described in Chapter IV.

Table 2. Personnel Controls—Dependent upon Program Administration and User Adherence to Policy

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| | | | | |
| Availability: Network security and user productivity | Protection and control of organizational network and data | Employees are prohibited from using organizational resources for accessing unauthorized content or conducting unauthorized activities | TTB<br>EEOC<br>CPG | AC-2<br>AC-2(E12)<br>AC-20(E3)<br>AU-14<br>CA-7<br>PL-4(E1)<br>SC-43<br>SI-4 |
| Confidentiality: unauthorized disclosure, control of data | Protection and control of organizational network and data | Technical solution allows access to organizational email through the Internet, but policy prohibits users from downloading organizational data to the personal side of the device | EEOC | AC-3(E9)<br>AC-20(E3)<br>SA-9 |
| Integrity & Confidentiality: Unauthorized access, unauthorized disclosure and modification | Secure remote authentication; protection and control of organizational network and data | Log off and disconnect from VPN when done working | TTB | AC-2(E5)<br>AC-20(E3)<br>PL-4<br>SC-10 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: Unauthorized disclosure and data control, privacy protection | Protection and control of organizational network and data | Protect PII. Do not download, email or transfer sensitive business data or PII to a personal device or any non-organizational device | TTB<br>EEOC (using GroupWise via the Internet)<br>CPG | AC-3(E9)<br>AC-20(E3)<br>AU-13<br>CA-7<br>IR-9<br>PL-4<br>SC-43<br>SI-4 |
| Confidentiality: Unauthorized disclosure, protection of data-at-rest | Protection and control of organizational network and data | Authorized storage of sensitive organizational information on an organizational approved device or removable media must be encrypted | TTB<br>CPG | AC-20(E3)<br>IA-5<br>MP-7<br>PL-4<br>SC-28(E1) |
| Confidentiality: Unauthorized disclosure and data control | Protection and control of organizational network and data | User agrees to delete any sensitive organizational files/data that may be inadvertently downloaded and stored on the device | EEOC<br>CPG | AC-3(E9)<br>AC-20(E3)<br>MP-6<br>PL-4 |
| Confidentiality: Access Control—principle of least privilege | Protection and control of organizational network and data | VPN access through BYOD is available to senior executives or management—must have CIO approval | EEOC | AC-2<br>AC-3<br>AC-6(E10)<br>AC-17<br>AC-19<br>AC-20(E3) |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: Access Control | Protection and control of organizational network and data | Users must have a need to access internal resources | TTB<br>EEOC | AC-2<br>AC-3<br>AC-6(E10)<br>AC-17<br>AC-19<br>AC-20(E3)<br>PS-6 |
| User safety | | Abide by the law governing the use of mobile cell phones and smartphones while driving | EEOC<br>CPG | AC-20(E3)<br>PL-4 |
| Availability and Confidentiality: unauthorized disclosure, data control | Protection and control of organizational network and data | Third party file sharing and Internet backup services, such as Dropbox and iCloud cannot be used to synchronize or backup company data | CPG | AC-20(E3)<br>AC-20(E4)<br>AU-14<br>CA-7<br>IR-9<br>PL-4<br>SC-43<br>SI-4 |
| Availability: data control | Protection and control of organizational network and data | All material that passes through the Company network or that is stored on Mobile Devices—including personally owned Mobile Devices—for the purpose of conducting business belongs to the Company | EEOC<br>CPG | AC-20(E3)<br>AU-2<br>AU-13<br>AU-14<br>CA-7<br>PL-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: data control and unauthorized disclosure | Protection and control of organizational network and data | Users must not employ any email address other than an official company email address to conduct company business | CPG | AC-20(E3)<br>IR-9<br>PL-4<br>SC-43<br>SI-4 |
| Confidentiality: unauthorized disclosure and OPSEC | Protection and control of organizational network and data | Inadvertent disclosure—be professional and exercise caution when using social networking, email, instant messaging services and chat rooms | TTB<br>CPG | AC-20(E3)<br>AU-13<br>CA-7<br>IR-6<br>IR-9<br>PL-4(E1)<br>SC-38<br>SC-43<br>SI-4 |
| Availability, Confidentiality and Integrity: unauthorized access, modification and protection of data-at- rest | Protection and control of organizational network and data | Do not access, browse, research, or change any account, file, data, record, or application not required to perform your official duties | TTB | AC-2<br>AC-5<br>AC-6<br>AC-20(E3)<br>AU-2<br>AU-14<br>CA-7<br>PL-4<br>SC-43<br>SI-4<br>SI-7 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Availability, Confidentiality and Integrity: data control, unauthorized disclosure, system and network security | Protection and control of organizational network and data | Privately owned equipment shall not be connected to organizational systems or networks | TTB | AC-20(E3)<br>CA-7<br>CA-9<br>MP-7<br>PL-4<br>SC-43<br>SI-4 |
| | | | | |

Table 3. Technical Controls—Technological Solutions that Enforce or Promote Compliance

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| | | | | |
| Confidentiality and Integrity: unauthorized disclosure or modification, protection of data-in- transit, privacy protection | Protection and control of organizational network and data | Sensitive data or PII must be encrypted prior to transmission | TTB | AC-20(E3)<br>IR-9<br>PL-4<br>SC-8(E1)<br>SC-43<br>SI-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Availability, Confidentiality and Integrity: unauthorized access, disclosure and modification, network security | Secure remote authentication; maintain device OS integrity; protection and control of organizational network and data | Do not install or use unauthorized hardware or software | TTB<br>CPG | AC-19<br>AC-20(E3)<br>CA-7<br>CM-2(E2)<br>CM-6(E2)<br>CM-7<br>CM-8(E3)<br>CM-11<br>IA-3<br>PL-4<br>SC-7<br>SC-43<br>SI-4<br>SI-7 |
| Availability and Confidentiality: Access control and network security | Secure remote authentication; protection and control of organizational network and data | Only use provided and properly configured equipment and software to remote access information networks, systems and data | TTB<br>EEOC | AC-17(E1, E6)<br>AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-8(E3)<br>CM-11<br>IA-3<br>PL-4<br>SC-7<br>SC-43<br>SI-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: Access control, unauthorized disclosure | Secure remote authentication; protection and control of organizational network and data | To establish a VPN connection the device must be capable of at least 128 bit encryption | TTB | AC-17(E2, E6)<br>AC-19<br>AC-20(E3)<br>IA-3<br>PL-4<br>PL-8<br>SC-8(E1)<br>SC-13<br>SC-28(E1)<br>SI-4 |
| Confidentiality and Integrity: Access control and authentication, unauthorized disclosure and modification | Protection and control of organizational network and data | User will password protect the device or use a PIN | TTB<br>EEOC<br>CPG | AC-20(E3)<br>IA-2<br>IA-5(E1)<br>PL-4 |
| Confidentiality and Integrity: access control, network security, protection of data-at-rest | Maintain device OS integrity, protection and control of organizational network and data | User agrees to maintain the original device OS and keep the device current | EEOC<br>CPG | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>CM-7<br>CM-8(E3)<br>CM-11<br>IA-3<br>PL-4<br>SC-3<br>SC-7<br>SC-43<br>SI-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality and Integrity: access control, network security and protection of data-at-rest | Maintain device OS integrity; protection and control of organizational network and data | User will not "jail break" the device | EEOC<br>CPG | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>CM-8(E3)<br>IA-3<br>PL-4<br>PS-8<br>SA-18(E2)<br>SC-3<br>SC-7<br>SC-43<br>SI-4<br>SI-7(E7) |
| Confidentiality and Integrity: Access control, unauthorized disclosure or modification | Protection and control of organizational network and data | Device wipe following set number of failed password or PIN attempts | EEOC<br>CPG | AC-7(E2)<br>AC-20(E3)<br>MP-6(E8)<br>PL-4<br>PL-8 |
| Confidentiality: Access control, authentication, unauthorized disclosure | Protection and control of organizational network and data | Users must comply with EEOC password policies (password strength, expiration and history) | EEOC | AC-20(E3)<br>IA-4<br>IA-5<br>PL-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality and Integrity: Access control, protection of data-at-rest and in-transit, network security | Protection and control of organizational network and data | Only BYODs that provide FIPS 140-2 device level encryption may be physically connected to EEOC PCs | EEOC | PL-4<br>AC-20(E3)<br>CA-9<br>CM-8(E3)<br>IA-3<br>PL-4<br>PL-8<br>SC-28(E1)<br>SI-4 |
| Confidentiality: Access control, authentication, unauthorized disclosure | Protection and control of organizational network and data | User will enable use of a second strong password for authentication upon connecting a BYOD to an EEOC PC | EEOC | AC-20(E3)<br>IA-2<br>IA-4<br>IA-5<br>PL-4 |
| Availability, Confidentiality and Integrity: Access control, network and host security, unauthorized disclosure and modification | Protection and control of organizational network and data | User will maintain anti-virus protection on the device | EEOC | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>CM-11<br>IA-3<br>PL-4<br>PL-8<br>SC-7<br>SI-3<br>SI-4 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Availability, Confidentiality and Integrity: Access control, network security | Protection and control of organizational network and data | Users must allow administrators to install an AV security suite on personal device | EEOC | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>IA-3<br>PL-4<br>PL-8<br>SC-7<br>SI-3 |
| Availability, Confidentiality and Integrity: Access control, network security, configuration management | Maintain device OS integrity and protection and control of organizational network and data | Users must allow administrators to install mobile device management tools on their personal device | EEOC | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>IA-3<br>PL-4<br>SC-7<br>SI-4 |
| Confidentiality and Integrity: Unauthorized disclosure or modification, physical security | Protection and control of organizational network and data | Location Services must be turned on to find a lost or stolen device | CPG | AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>CM-8(E8)<br>IA-3<br>PE-20<br>PL-4<br>SC-42(E2) |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality and Integrity: Access control, unauthorized disclosure or modification, network security, configuration management | Maintain device OS integrity; protection and control of organizational network and data | Do not tamper with enabled security configurations—security settings will be enforced by the mobile device management client on all mobile devices that contain company data or have access to company systems | TTB<br>CPG | AC-19<br>AC-20(E3)<br>CM-2(E2)<br>CM-6(E2)<br>CM-8(E3)<br>IA-3<br>PL-4<br>PS-8<br>SA-9<br>SA-18(E2)<br>SC-3<br>SC-7<br>SC-43<br>SI-4<br>SI-7(E7) |
| Confidentiality and Integrity: Access control, unauthorized disclosure or modification, network security | Protection and control of organizational network and data | Device lock after 15 minutes of inactivity | CPG | AC-2(E5)<br>AC-11<br>AC-20(E3)<br>SC-10 |
| Confidentiality and Integrity: Access control, unauthorized disclosure or modification, protection of data-at-rest | Protection and control of organizational network and data | Devices will have the capability to initiate remote wipe if lost or stolen | EEOC<br>CPG | AC-20(E3)<br>CM-6(E2)<br>IA-3<br>IR-9<br>MP-6(E8)<br>PL-8 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: Access control, device accountability | Secure Remote Authentication; Protection and control of organizational network and data | Only Apple iOS iPad devices are allowed to establish VPN connections | EEOC | AC-19<br>AC-20(E3)<br>CM-8(E3)<br>IA-3<br>SI-4 |
| Cost management, device accountability, access control | Protection and control of organizational network and data | Termination of service due to 30 consecutive days of non-use | EEOC | AC-2(E3)<br>AC-20(E3)<br>SC-43 |
| Confidentiality and Integrity: Access control, authentication and non-repudiation | Secure remote authentication | Authentication to the organizational VPN requires two factors: RSA secure ID code and PIN | TTB | AC-17(E9)<br>AC-20(E3)<br>IA-2(E2)<br>IA-4<br>IA-5 |
| Confidentiality and Integrity: Unauthorized disclosure or modification, network security | Protection and control of organizational network and data | Technical controls prevent employees from saving any data either from or onto a local computer while connected to the VPN;<br>*Container prevents the transfer of organizational data outside the container or the transfer of personal data into the container | TTB<br>*EEOC (when using TouchDown container) | AC-3(E9)<br>AC-4(E22)<br>AC-20(E3)<br>SA-9<br>SC-4<br>SC-25 |
| Confidentiality: Access control, device management and accountability | Protection and control of organizational network and data | Only Android, iOS and BlackBerry devices are allowed within BYOD program | EEOC | AC-19<br>AC-20(E3) |
| | | | | |

Table 4. Operating Controls—Procedures and Processes to Resolve BYOD Incidents

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| | | | | |
| Availability, Confidentiality and Integrity: Unauthorized disclosure or modification, network security, physical security, insider threat | Secure remote authentication; maintain device OS integrity; protection and control of organizational network and data | Promptly report all security incidents regardless of how insignificant they may appear to include suspicious activity and possible disclosure of sensitive information | TTB<br>CPG | AC-2(E13)<br>AC-3(E9)<br>AC-20(E3)<br>AT-3(E4)<br>IA-5<br>IR-6<br>IR-9<br>PL-4 |
| Confidentiality: Unauthorized access | Secure remote authentication; protection and control of organizational network and data | Report loss of RSA Secure ID | TTB | AC-17(E6)<br>AC-20(E3)<br>IA-5<br>IR-6<br>PL-4<br>SC-10 |
| Confidentiality, Integrity: Unauthorized access, disclosure or modification | Protection and control of organizational network and data | Report lost or stolen device | TTB<br>EEOC<br>CPG | AC-20(E3)<br>IR-6<br>IR-9<br>PL-4 |
| Integrity: Data discovery, unauthorized modification or removal of data | Protection and control of organizational network and data | Legal hold—the organization may need to access all data stored on a device; user must get company approval prior to transferring or deleting contents | EEOC<br>CPG | AC-20(E3)<br>IR-9<br>PL-4<br>PS-8<br>SC-43 |

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Availability, Confidentiality and Integrity: Unauthorized access, disclosure or modification, network security | Secure remote authentication; maintain device OS integrity; protection and control of organizational network and data | Notify the company if a local government agency or outside organization seizes your mobile device. Device must be inspected prior to resuming use | TTB<br>CPG | AC-20(E3)<br>AT-3(E2)<br>CM-2(E7)<br>IR-6<br>PL-4<br>SA-18(E2) |
| Confidentiality and Integrity: Access control, unauthorized disclosure or modification, device accountability | Protection and control of organizational network and data | Remote wipe as a result of separation from the company | CPG | AC-2<br>AC-20(E3)<br>MP-6(E8)<br>PL-4<br>PS-4<br>PS-5 |
| Confidentiality, Integrity: Access control, unauthorized disclosure or modification | Secure remote authentication; protection and control of organizational network and data | Employees may not make any remote connection via TTB's VPN to any TTB network resource while outside the United States | TTB | AC-17(E1, E6)<br>AC-19<br>AC-20(E3)<br>CM-2(E7)<br>CM-8(E3)<br>IA-3<br>PL-4<br>SC-7<br>SC-43<br>SI-4 |
| | | | | |

Table 5. Physical Controls—Actions Required by User to Ensure the Physical Protection of the Device and Resident Data

| Security Objective/Concern Addressed | USMC Security Requirement Supported | Case Study Security Capabilities/Controls | Case Study Organization | SP-800-53 Controls |
|---|---|---|---|---|
| Confidentiality: Authentication, unauthorized disclosure, logical access control | Secure remote authentication; maintain device OS integrity; protection and control of organizational network and data | Protect all authentication credentials (RSA secure ID, username and password or PIN) | TTB<br>CPG | AC-20(E3)<br>IA-5<br>PL-4 |
| Confidentiality and Integrity: Authentication, unauthorized disclosure or modification, logical access control | Secure remote authentication; maintain device OS integrity; protection and control of organizational network and data | Do not program your authentication credentials to be input automatically | TTB<br>CPG | AC-20(E3)<br>AT-3(E2)<br>IA-5<br>PL-4 |
| Confidentiality and Integrity: Unauthorized access disclosure or modification, physical security | Protection and control of organizational network and data | Personnel should take every precaution to physically protect device—Examples include: locking in a safe if on travel, keeping it on your person, do not leave in locked car unattended, etc. | TTB<br>CPG | AC-20(E3)<br>AT-3(E2)<br>PL-4 |
| Confidentiality and Integrity: Unauthorized disclosure or modification, physical and logical access control, physical security | Maintain device OS integrity; protection and control of organizational network and data | User will not share the device with other individuals or family members | EEOC | AC-20(E3)<br>AT-3(E2)<br>PL-4<br>SC-43 |

Table 6 includes each unique SP-800-53 security control that aligned with at least one policy standard from the case study organizations' BYOD policies (column five from the above tables). These controls are highlighted in yellow. The SP-800-53 controls that are not highlighted have been identified as having applicability to the USMC BYOD program, but did not align with any of the policy standards listed in the case study user agreements. This table is not meant to be an inclusive list of all the security controls required to minimize risk within a BYOD program. Rather, it lists those security controls from the SP-800-53 that either technically enforce a participant's acceptable use of a personally owned device within a BYOD program, or are recommended in this thesis for inclusion within a user agreement to minimize risk due to personal use of a dual-use device in conjunction with the MCEN.

At the time of this research, the FIPS-199 impact levels assigned to the USMC BYOD program and the MCEN were not readily available. Per NIST, a system is assigned an impact level of low, moderate, or high, and is based on the "impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals."[315] Based on the findings of this research, the USMC BYOD program should be assigned an impact level of moderate or higher. The identified SP-800-53 security controls listed below have been matched to the appropriate impact level, so that as the USMC identifies the impact level of the BYOD program, a viable baseline of BYOD security controls is available and tailored to the USMC BYOD technological solution. As per the SP-800-53, an "X" indicates the associated security control is required as a baseline to meet the identified impact level (i.e., low, moderate, high). If the cell is blank, the security control or control enhancement is not required for the security control baseline, but is available for increased protection. To reiterate, the identified controls in Table 6 are primarily applicable to the user experience, procedures, and processes in the formulation of user agreements vice an all-inclusive list of controls

[315] National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems*, 1.

required for BYOD implementation. The SP-800-53 and SP-800-124 should be referenced for a complete list of required security controls.

Table 6. Security Control Baseline for BYOD Impact Level[316]

| SP-800-53 Control Number | Control or Control Enhancement name | Impact Level | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| **AC-2** | **Account Management** | **X** | **X** | **X** |
| **AC-2(E3)** | Disable Inactive Accounts | | **X** | **X** |
| **AC-2(E5)** | Inactivity Logout | | | **X** |
| **AC-2(E11)** | Usage Conditions | | | **X** |
| **AC-2(E12)** | Account Monitoring/Atypical Usage | | | **X** |
| **AC-2(E13)** | Disable Accounts for High-Risk Individuals | | | **X** |
| **AC-3** | **Access Enforcement** | **X** | **X** | **X** |
| **AC-3(E9)** | Controlled Release | | | |
| **AC-4** | **Information Flow Enforcement** | | **X** | **X** |
| **AC-4(E22)** | Access Only | | | |
| **AC-5** | **Separation of Duties** | | **X** | **X** |
| **AC-6** | **Least Privilege** | | **X** | **X** |
| **AC-6(E10)** | Prohibit Non-Privileged Users from Executing Privileged Functions | | **X** | **X** |
| **AC-7** | **Unsuccessful Logon Attempts** | **X** | **X** | **X** |
| **AC-7(E2)** | Purge/Wipe Mobile Devices | | | |
| **AC-8** | **System Use Notification** | **X** | **X** | **X** |
| **AC-11** | **Session Lock** | | **X** | **X** |
| **AC-12** | **Session Termination** | | **X** | **X** |
| **AC-17** | **Remote Access** | **X** | **X** | **X** |

316 Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, D1–D43.

| SP-800-53 Control Number | Control or Control Enhancement name | Impact Level | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| **AC-17(E1)** | Automated Monitoring/Control | | **X** | **X** |
| **AC-17(E2)** | Protection of Confidentiality/Integrity Using Encryption | | **X** | **X** |
| **AC-17(E6)** | Protection of Information | | | |
| **AC-17(E9)** | Disconnect/Disable Access | | | |
| **AC-19** | **Access Control for Mobile Devices** | **X** | **X** | **X** |
| **AC-19(E4)** | Restrictions for Classified Information | | | |
| **AC-19(E5)** | Full Device/Container-Based Encryption | | **X** | **X** |
| **AC-20** | **Use of External Information Systems** | **X** | **X** | **X** |
| **AC-20(E3)** | Non-Organizationally Owned Systems/Components/Devices | | | |
| **AC-20(E4)** | Network Accessible Storage Devices | | | |
| **AC-22** | **Publicly Accessible Content** | **X** | **X** | **X** |
| **AT-2** | **Security Awareness Training** | **X** | **X** | **X** |
| **AT-3** | **Role-Based Security Training** | **X** | **X** | **X** |
| **AT-3(E2)** | Physical Security Controls | | | |
| **AT-3(E4)** | Suspicious Communications and Anomalous System Behavior | | | |
| **AU-2** | **Audit Events** | **X** | **X** | **X** |
| **AU-13** | **Monitoring for Information Disclosure** | | | |
| **AU-14** | **Session Audit** | | | |
| **CA-7** | **Continuous Monitoring** | **X** | **X** | **X** |
| **CA-9** | **Internal System Connections** | **X** | **X** | **X** |
| **CM-2** | **Baseline Configuration** | **X** | **X** | **X** |
| **CM-2(E2)** | Automation Support for | | | **X** |

| SP-800-53 Control Number | Control or Control Enhancement name | Impact Level | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| | Accuracy/Currency | | | |
| **CM-2(E7)** | Configure Systems, Components, or Devices for High-Risk Areas | | **X** | **X** |
| **CM-6** | **Configuration Settings** | **X** | **X** | **X** |
| **CM-6(E2)** | Respond to Unauthorized Changes | | | **X** |
| **CM-7** | **Least Functionality** | **X** | **X** | **X** |
| **CM-7(E4)** | Unauthorized Software/Blacklisting | | **X** | |
| **CM-7(E5)** | Authorized Software/Whitelisting | | | **X** |
| **CM-8** | **Information System Component Inventory** | **X** | **X** | **X** |
| **CM-8(E3)** | Automated Unauthorized Component Detection | | **X** | **X** |
| **CM-10** | **Software Usage Restrictions** | **X** | **X** | **X** |
| **CM-11** | **User-Installed Software** | **X** | **X** | **X** |
| **CM-11(E1)** | Alerts for Unauthorized Installations | | | |
| **IA-2** | **Identification and Authentication** | **X** | **X** | **X** |
| **IA-2(E2)** | Network Access to Non-Privileged Accounts | | **X** | **X** |
| **IA-3** | **Device Identification and Authentication** | | **X** | **X** |
| **IA-4** | **Identifier Management** | **X** | **X** | **X** |
| **IA-5** | **Authenticator Management** | **X** | **X** | **X** |
| **IA-5(E1)** | Password-Based Authentication | **X** | **X** | **X** |
| **IA-5(E2)** | PKI-Based Authentication | | **X** | **X** |
| **IA-5(E3)** | In-Person or Trusted Third-Party Registration | | **X** | **X** |
| **IA-5(E4)** | Automated Support for Password Strength Determination | | | |

| SP-800-53 Control Number | Control or Control Enhancement name | Impact Level | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| **IA-5(E11)** | Hardware Token-Based Authentication | **X** | **X** | **X** |
| **IR-6** | **Incident Reporting** | **X** | **X** | **X** |
| **IR-9** | **Information Spillage Response** | | | |
| **MA-2** | **Controlled Maintenance** | **X** | **X** | **X** |
| **MP-6** | **Media Sanitization** | **X** | **X** | **X** |
| **MP-6(E8)** | Remote Purging/Wiping of Information | | | |
| **MP-7** | **Media Use** | **X** | **X** | **X** |
| **PE-20** | **Asset Monitoring and Tracking** | | | |
| **PL-4** | **Rules of Behavior** | **X** | **X** | **X** |
| **PL-4(E1)** | Social Media and Networking Restrictions | | **X** | **X** |
| **PL-8** | **Information Security Architecture** | | **X** | **X** |
| **PS-1** | **Personnel Security Policy and Procedures** | **X** | **X** | **X** |
| **PS-3** | **Personnel Screening** | **X** | **X** | **X** |
| **PS-4** | **Personnel Termination** | **X** | **X** | **X** |
| **PS-5** | **Personnel Transfer** | **X** | **X** | **X** |
| **PS-6** | **Access Agreements** | **X** | **X** | **X** |
| **PS-7** | **Third-Party Personnel Security** | **X** | **X** | **X** |
| **PS-8** | **Personnel Sanctions** | **X** | **X** | **X** |
| **SA-9** | **External Information System Services** | **X** | **X** | **X** |
| **SA-18** | **Tamper Resistance and Detection** | | | |
| **SA-18(E2)** | Inspection of Information Systems, Components, or Devices | | | |

| SP-800-53 Control Number | Control or Control Enhancement name | Impact Level | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| **SC-3** | **Security Function Isolation** | | | **X** |
| **SC-4** | **Information in Shared Resources** | | **X** | **X** |
| **SC-7** | **Boundary Protection** | **X** | **X** | **X** |
| **SC-7(E7)** | Prevent Split Tunneling for Remote Devices | **X** | **X** | **X** |
| **SC-8** | **Transmission Confidentiality and Integrity** | | **X** | **X** |
| **SC-8(E1)** | Cryptographic or Alternate Physical Protection | | **X** | **X** |
| **SC-10** | **Network Disconnect** | | **X** | **X** |
| **SC-13** | **Cryptographic Protection** | **X** | **X** | **X** |
| **SC-25** | **Thin Nodes** | | | |
| **SC-28** | **Protection of Information at Rest** | | **X** | **X** |
| **SC-28(E1)** | Cryptographic Protection | | **X** | **X** |
| **SC-38** | **Operations Security** | | | |
| **SC-41** | **Port and I/O Device Access** | | | |
| **SC-42(E2)** | Authorized Use | | | |
| **SC-43** | **Usage Restrictions** | | | |
| **SI-3** | **Malicious Code Protection** | **X** | **X** | **X** |
| **SI-4** | **Information System Monitoring** | **X** | **X** | **X** |
| **SI-7** | **Software, Firmware, and Information Integrity** | | **X** | **X** |
| **SI-7(E2)** | Automated Notifications of Integrity Violations | | | **X** |
| **SI-7(E7)** | Integration of Detection and Response | | **X** | **X** |
| **SI-7(E9)** | Verify Boot Process | | | |

Other than a few exceptions, the security controls in the SP-800-53 catalog, "have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission."[317] Simply because a control is listed in the SP-800-53, or identified in a case study user policy, does not mean that it should be included in the USMC policy. For this reason, understanding the technology that the policy is designed to support is vital so that the implemented controls are both meaningful and relevant.[318] Furthermore, the need to provide sufficient security extends beyond the implementation of any one safeguard associated with a particular technology. The recommended safeguards or controls provided in Appendix B (the proposed USMC BYOD user agreement) in support of the USMC BYOD program have been analyzed based on the methodology described in Chapter IV for their applicability to support the technological solutions under evaluation by the USMC.

[317] Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.), *Security and Privacy Controls for Federal Information Systems and Organizations*, ix.

[318] Ibid.

# APPENDIX B. PROPOSED BRING-YOUR-OWN-DEVICE USER AGREEMENT

## BYOD User Agreement

## UNITED STATES MARINE CORPS BRING-YOUR-OWN-DEVICE (BYOD) USER AGREEMENT

**PURPOSE & OBJECTIVE:**

The United States Marine Corps (USMC) Bring Your Own Device (BYOD) program allows for the use of an approved commercial mobile device (CMD) of the employee's choice to access Marine Corps Enterprise Network (MCEN) resources. The BYOD program intends to reduce costs associated with the issuance of Government Furnished Equipment (GFE) while fostering enhanced productivity as it allows participants to access, disseminate and manipulate USMC and U.S. Government data from non-traditional work places in order to support mission requirements. As such, this document establishes the USMC's policy regarding acceptable use of personally-owned mobile devices within the BYOD program.

This BYOD agreement aims to inform BYOD participants of their responsibilities as well as the potential consequences if guidelines contained within this agreement are not followed. Furthermore, this agreement seeks to minimize risk to our people, the MCEN and the data it contains by establishing acceptable use practices for conducting work and while connected to the MCEN via your mobile device. Failure to adhere to the guidelines listed in this agreement may result in disciplinary action, personal liability and termination of BYOD privileges.

**A commercial mobile device** is a handheld computing device with a display screen that allows for user input (e.g., touch screen, keyboard). When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information, given device limitations (i.e., screen size, computing power). Mobile devices provide the capabilities of conventional desktops or laptop computers in a more portable package. Examples of popular mobile devices include smart phones and tablets. Mobile devices approved for use in this BYOD program are provided at https://aplits.disa.mil/processAPList.action—type "mobile device" into the "key words" search field.

**The Organizational Container** present on a personally-owned mobile device is owned by the United States Marine Corps. This container securely partitions the device to ensure that organizational data and work related functions remain separate and isolated from the personal side of the device, thus creating a dual-use capability that helps address both security and user privacy concerns.

**Organizational Data** is the property of the U.S. Federal Government and consists of any data accessed, stored, manipulated, processed or transmitted within or through the organizational container.

**Remote Wipe:** Devices must have the capability to receive a remote command to perform a remote wipe. In the event of a lost or stolen device and the transfer or termination of employment, the USMC will initiate a remote wipe to erase only the organizational container resident on the personally-owned device.

**Legal Hold** is a process that permits the U.S. Federal Government to preserve all forms of relevant information as a result of current or anticipated litigation, audit or government investigation. In the event of a court ordered legal hold for data discovery, a BYOD participant is required to preserve all documents and electronically stored information (ESI) associated with an investigation, lawsuit, or audit.

**SCOPE:**

This agreement applies to any employee (military, civilian and contractor) who decides to participate in this BYOD program and uses a personally-owned mobile device to access MCEN resources and services. Individuals covered by this agreement are referred to as Mobile Device Users or BYOD participants. This program is voluntary and offered to all full-time employees. No employee should be pressured into participating and only individuals identified as "mission essential" personnel are given the expectation of being contactable outside of existing work patterns.

**PRIVACY:**

Employees assume some level of risk by participating in this BYOD program. The USMC will NOT violate an individual's right to privacy associated with personal use of the device while conducting activities outside of the organizational container, unless a violation of this agreement is suspected or detected.

1. The USMC will not and cannot remotely access personal data on an employee's personally-owned device residing outside of the Organizational Container.

2. Monitoring: BYOD participants shall use the Organizational Container and associated MCEN resources with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

Activities conducted on the personal side of a device shall utilize commercial Internet or cellular service to send and receive traffic. Therefore, activities conducted outside of the organizational container are not monitored or seen by the USMC.

3. Remote Wiping: When a Remote wipe command is required, it is designed to erase only the data residing in the Organizational Container without affecting any personal data outside of the container.

**STANDARDS:**

This acceptable use policy (AUP) has been generated in accordance with applicable laws and regulations and must be adhered to in order to protect employees, the organization, networks and data. Appropriate use of Federal Government communications systems and electronic media in accordance with DOD Directives, Instructions and regulations also apply while using the organizational container resident on a personally-owned mobile device.

Mobile Device Users are responsible for protecting U.S. Government data, keeping the device itself secure, immediately reporting security incidents and the loss or theft of devices, allowing BYOD administrators to remote wipe (delete) the organizational container as required, and to access the organizational container for data discovery in the event of a legal hold or spillage of classified data.

Participation in the USMC BYOD program is granted on the condition that an individual:

(1) has a requirement to access USMC resources;
(2) completes applicable training requirements;
    (a) DOD Information Assurance Awareness Training;
    (b) Personal Identifiable Information Training;
    (c) Smartphones and Tablets Appropriate Use modules;
    (d) Portable Electronic Devices & Removable Storage Media training.
(3) submits a BYOD System Access Authorization Request (SAAR);
(4) reads, signs and adheres to the BYOD acceptable use policies as described in this document.

Additional standards and controls specific to the use of personally-owned mobile devices within the USMC BYOD program are identified in this agreement.

**PERSONNEL CONTROLS are dependent upon program administration and user adherence to this agreement.**

1. Only unclassified official business shall be conducted within the organizational container and while connected to the MCEN. BYOD participants are prohibited from accessing unauthorized content (such as pornography, hacker sites, and gambling sites) via the USMC organizational container and virtual private network (VPN) connection.

2. If a BYOD participant is suspected of using his/her personally-owned mobile device to conduct illegal activity or to access unauthorized content via the VPN connection, the organizational container will be locked and BYOD privileges will be terminated. Suspected illegal activity will be reported to appropriate civil authorities and the participant's device could be confiscated as evidence.

3. Use of the organizational container on a personally-owned device is subject to the same policies as using an unclassified U.S. Government IT resource and is not authorized

to access, store or transmit classified data or otherwise unauthorized content. Personally-owned mobile devices shall not be used to discuss classified information.

4. Reasonable personal use of a mobile device during working hours is allowed but it shall not interfere with organizational activities or the employee's official responsibilities. Excessive personal use of a mobile device during working hours for other than official or authorized use may result in adverse administrative or disciplinary action. Personal use of a mobile device should be conducted outside of the organizational container and during the employee's personal time (i.e. during lunch periods, official breaks, or outside of normal working hours).

5. Do not access, browse, research, or change any account, file, data or application outside the scope of assigned duties.

6. BYOD participants must disconnect the remote session and log out of the organizational container when work will be interrupted for more than five minutes. BYOD participants must also lock the device when not in use.

7. Do not employ any email address to conduct official business other than an official USMC email address.

8. Do not physically connect or synchronize personally-owned mobile devices to a government system. Participants are responsible for periodically backing up organizational data resident within the organizational container to the MCEN.

9. Terminate the VPN connection and log out of the organizational container prior to connecting the personally-owned device to another personally-owned device (e.g., personal computer, storage or any other external device).

10. Do not attempt to synchronize, backup or transfer government data to non-government systems, mobile devices, third party file sharing services or cloud based storage services, such as iCloud and Dropbox. Do not email government information to a personal email account (i.e., Gmail, Hotmail, Yahoo, etc.) in an attempt to bypass this control.

11. BYOD participants are legally liable for posted content on the Internet (which includes social media sites) and can be disciplined by the USMC for commentary, content or images that are defamatory, pornographic, proprietary, harassing, libelous or that can create a hostile work environment. Utilizing a personally-owned mobile device within the workplace to access vulgar content or content that could otherwise be interpreted as offensive is prohibited. Standing Equal Employment Opportunity (EEO) and sexual assault/harassment policies apply.

12. Be professional and exercise caution when using social networking, email, instant messaging and chat rooms as lapses can result in unauthorized disclosures of sensitive information and operations security (OPSEC) violations.

13. Unless authorized, BYOD participants will not post organizational content online.

14. Overtime compensation is not available simply because a BYOD participant utilizes a personally-owned device to conduct work after hours. If overtime is required based on work performed via a personally-owned device outside of normal working hours, BYOD participants must first obtain authorization from a supervisor.

15. Personally-owned mobile devices are not allowed in areas where classified information is stored, processed, discussed or transmitted.

16. BYOD participants will abide by the law governing the use of mobile devices while driving or conducting any other activity covered by legal restrictions. Where legally approved, the use of hands-free equipment is recommended.

**TECHNICAL CONTROLS enforce or promote compliance to this agreement through technological capabilities.**

1. BYOD participants must register their personally-owned mobile device with USMC BYOD administrators through the submission of a SAAR. The participant will then download the container application from the appropriate application store (e.g. Apple Store for iOS devices). BYOD administrators will email the participant an enterprise activation code, as well as guidance to properly configure the personally-owned device. The container application and device security settings are required for remote authentication and access to the MCEN. If the device is not properly configured, access to the MCEN will not be allowed.

2. Do not alter or tamper with enabled security configurations. Technical solutions are in place to detect configuration changes and enforce proper settings. Mobile devices outside of acceptable risk parameters will not be allowed access to the organizational container until the proper settings are reestablished.

3. A PIN (or similar access mechanism depending on the type of device) is required to unlock the personally-owned device.

4. A username and password is required to access the organizational container. The password required to access the organizational container must be changed every 90 days and comply with DOD complexity requirements.

5. Mobile device users will comply with DOD password and PIN policies. PINs and passwords must be protected and the PIN required to establish a VPN connection will be different from the PIN necessary to access the device. Do not make an attempt to bypass access control measures.

6. Authentication to the USMC VPN requires two factors. In order to establish a VPN connection, users must have derived credentials loaded in the organizational container and the associated PIN. The VPN connector and derived credentials will be installed

within the organizational container on the BYOD participant's device following the review and signature of this agreement and the submission of a SAAR.

7. The organizational container will be locked and the VPN connection will be automatically disconnected following five minutes of inactivity. This does not excuse the user from logging out of the organizational container and disconnecting the remote session when work will be interrupted for more than five minutes. The device itself will also be set to lock after one minute of inactivity.

8. The ability to establish a VPN connection will be disabled following five unsuccessful attempts to enter the correct PIN. Similarly, access to the organizational container will be locked following five unsuccessful login attempts. In both cases, BYOD administrators must be contacted to unlock the account and reestablish access.

9. Do not modify or use unauthorized mobile device hardware.

10. Do not install or use unauthorized software within the organizational container. Unauthorized software includes, but is not limited to, hacking tools, opt-in botnet software and other attack tool technologies, peer-to-peer software (e.g. Napster, LimeWire), and non-business related third-party applications. Applications authorized for use within the organizational container are available for download from approved enterprise application stores only.

11. Sensitive U.S. Government data and Personally Identifiable Information (PII) stored or processed on a personally-owned mobile device must be encrypted. Such information must also be encrypted prior to transmission. All data stored within the organizational container is automatically encrypted. Any effort to circumvent this encryption is strictly prohibited.

12. The BYOD participant is responsible for promptly applying available patches and maintaining proper configuration settings. BYOD participants agree to maintain the original device operating system (OS).

13. BYOD participants will not attempt to root or jailbreak any mobile device utilized within the USMC BYOD program. Rooting or jailbreaking a device means that the user bypasses security restrictions to elevate user privileges to alter device settings, install otherwise unauthorized third-party software and applications, as well as modify the OS and file systems. Technical solutions are in place to detect a compromised OS. Any attempt to root or jailbreak a device will, at a minimum, result in the termination of BYOD privileges and a remote wipe of the organizational container.

14. Technical controls are in place to prevent the transfer of organizational data from the organizational container to the personal side of the device and vice versa. Do not attempt to circumvent this separation.

15. BYOD participant accounts that go unused for 30 consecutive days will be locked. If no attempts are made to unlock the organizational container for an additional 30 days, a

remote wipe of the organizational container will be initiated. Employees must re-enroll if they decide to continue participation in the future.

**<u>OPERATING CONTROLS</u> provide the procedures and processes to manage device accountability and prevent or resolve BYOD incidents.**

1. BYOD participants will promptly report all security incidents regardless of how insignificant they may appear. Security incidents include, but are not limited to: suspicious activity; anomalous or erratic device operation; missing or added files; the possible disclosure of sensitive but unclassified information (i.e. PII and OPSEC data); and the spillage of classified information.

2. Report lost or stolen devices immediately to the Marine Corps Enterprise helpdesk.

3. Be aware of social engineering and phishing attempts. Exercise caution before clicking on Internet links or opening attachments from an unknown source or included within emails that are not digitally signed.

4. Exercise caution when conducting work on a personally-owned mobile device. Information transmitted via a personally-owned device (e.g. email, the Internet and telephone) may be accessible by anyone else on the network. BYOD participants must be careful when utilizing email distribution lists. Ensure recipient(s) are authorized and have a need-to-know prior to transmitting sensitive data.

5. BYOD participants may not use personally-owned mobile devices to establish VPN connections while outside the U.S., Canada or U.S. Territories. For travel outside of these areas associated with official business, government furnished devices will be provided. When possible, BYOD participants should notify BYOD administrators at least two weeks prior to travel (or as soon as possible) to facilitate the issuance of a government furnished device.

6. Prior to OCONUS leisure travel, BYOD participants must notify BYOD administrators. For security purposes the organizational container will be deactivated for the duration of OCONUS leisure travel.

7. BYOD participants will notify BYOD administrators if an outside agency or organization seizes the personally-owned mobile device for any period of time, or if a lost device is suddenly found. The device must be inspected prior to resuming use of the organizational container.

8. Immediately report compromised VPN or organizational container credentials to BYOD administrators so that they can be changed. BYOD participants will immediately reset the PIN required to access the device if a compromise is suspected.

9. The transfer or separation of BYOD participants will be reported to personnel administration and BYOD administrators who will initiate a remote wipe of the organizational container and terminate remote access capabilities on the date of

detachment. The participant can enroll in the BYOD program (if offered) at the gaining organization. If organizational data stored within the organizational container is necessary for the BYOD participant's follow-on assignment, the BYOD participant is responsible for coordinating with BYOD administrators in accordance with check-out procedures.

10. BYOD participants must coordinate with USMC BYOD administrators prior to trading in or transferring ownership of a personally-owned device. This process ensures device accountability within the BYOD program and the removal of the organizational container prior to device trade-in or transfer. Contents of the organizational container and its contents will be saved by BYOD administrators and available for downloaded to the new device following the submission of an updated SAAR and enrollment of the new device.

11. The USMC does not pay for BYOD participants to buy, operate, repair or support personally-owned mobile devices. BYOD participants are responsible for all costs related to personally-owned mobile devices, except for the management and maintenance associated with the organizational container. BYOD participants will have personally-owned mobile devices inspected to ensure proper configuration and ensure there are no signs of physical tampering following maintenance performed by third-party service providers.

12. Unless authorized, BYOD participants are allowed to register and utilize only one device within the USMC BYOD program.

13. Separate policy guidance will be generated in the event of a government furlough.

**PHYSICAL CONTROLS are those actions required by BYOD participants to ensure the physical protection of the device and resident data.**

1. Protect all authentication credentials. Do not write down passwords and PINs or store them on a personally-owned device. Do not program your authentication credentials to be entered automatically. To prevent others from obtaining user passwords and PINS, BYOD participants will shield the device screen while entering credentials. Do not share PINs, usernames or passwords with anyone, regardless of their position of authority.

2. BYOD participants should take every precaution to physically protect their device against loss, theft, damage, abuse and unauthorized use. Common best practices include:

(a) Maintain physical control of the device
(b) If the device must be left unattended, lock it in a drawer or cabinet
(c) Do not leave devices unattended in a locked car
(d) Whether on personal or business travel, never include mobile devices with checked luggage or with a hotel baggage service
(e) Lock the device in a safe while on travel

3. Ensure you are logged out of the organizational container prior to sharing the device with other individuals or family members. Use of the device by another individual should be of short duration and supervised.

4. Be aware of your surroundings when discussing potentially sensitive topics while in public areas.

**COMPLIANCE:**

1. By signing this document, the BYOD participant acknowledges that they have read, acknowledged and signed DD Form 2875, System Authorization Access Request (U.S. Marine Corps) and the associated addendum, which outlines the mandatory DOD standard consent provision and Navy and Marine Corps' user responsibilities when accessing Department of Defense (DOD) information systems and resources.

2. User agrees to complete annual BYOD training requirements in addition to reading, signing and submitting a new BYOD user agreement.

3. The USMC is not liable for any personal use of personally-owned mobile devices or for any personal data stored on devices outside of the organizational container.

4. The USMC is not responsible for loss, defects, failures, unauthorized use, or violation of applicable policy or damage of or associated with personally-owned mobile devices.

5. BYOD participant is the only authorized user of an assigned user account and will be held responsible for any and all activity that occurs while logged into the organizational container with the assigned credentials.

6. Violations to this agreement determined to be purposeful or repeated as a result of BYOD participant negligence will be documented in employee evaluations and Joint Personnel Adjudication System (JPAS) when applicable.

Conduct which does not conform to these acceptable use guidelines may form the basis for appropriate disciplinary action. Penalties can range from reprimand and revocation of BYOD privileges for a minor infraction to removal from the Federal Service or criminal prosecution for the most serious violations. Employees are required to acknowledge these acceptable use guidelines prior to being granted BYOD access privileges.

---

*I, the undersigned, acknowledge that I have read this document and understand the terms of use and my responsibilities as an authorized USMC BYOD program participant. I agree to these terms in their entirety and will comply to the best of my ability at all times. I accept these terms freely and voluntarily of my own accord. I make no claims on my employer to protect any personal data that may reside on my personally-owned device, and I understand that any violation of these BYOD Acceptable Use Standards may be cause for revocation of BYOD eligibility and/or disciplinary action.*

**BYOD User's Name (Typed or Printed):**_____

**Title or Rank:**_____

**Office or Department:**_____

**Official Email Address:**_____

**Telephone Number (Work and Mobile):** _____

**BYOD User's Signature:** _____

**Date of Signature:** _____

# LIST OF REFERENCES


Alcohol and Tobacco Tax and Trade Bureau. *Remote Access Policy*. (7320.1G). Washington, DC: Alcohol and Tobacco Tax and Trade Bureau, 2011.

———. *TTB IT Security Rules of Behavior*. Washington, DC: Alcohol and Tobacco Tax and Trade Bureau TTB, n.d.

Android. "Encryption." Accessed December 20, 2014. https://source.android.com/devices/tech/security/encryption/Android.

Azuri, Calvin. "Samsung KNOX Hypervisor Receives Approval for Use by U.S. Department of Defense." *TMCnet.com*, March 18, 2014. http://technews.tmcnet.com/channels/enterprise-mobile-solutions/articles/373702-samsung-knox-hypervisor-receives-approval-use-us-department.htm.

Blackberry.com. "Secure Work Space for iOS and Android." Accessed December 30, 2014. http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/bfb/Secure-Work-Space-datasheet.pdf.

Boland, Rita. "Pocket to Payload, Personal Technologies Serve the Marine Corps Environment." *Signal Online*, April 1, 2014. http://www.afcea.org/content/?q=node/12513.

Cassavoy, Liane. "What Does It Mean to Jailbreak an iPhone?" *About Technology*. Accessed June 4, 2014. http://cellphones.about.com/od/glossary/f/jailbreak_faq.htm.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone, and National Institute of Standards and Technology (U.S.). *Computer Security Incident Handling Guide*. (NIST Special Publication (SP) 800-61 Revision 2). Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2012. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

Command, Control, Communications, and Computers Department (C4). *Marine Corps Commercial Mobile Device Strategy*. Washington, DC: Headquarters, U.S. Marine Corps, 2013. http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/20130411_Marine_Corps_Commercial_mobile_device_strategy_Final.pdf.

Common Criteria for Information Technology Security Evaluation, Version 3.1. CCIMB-2012-09-[001, 002, 003] Common Criteria Project Sponsoring Organizations, January 2012.

Corsec Security, Inc. *AT&T Toggle Cryptographic Security Module, Software Version: 1.0, FIPS 140-2 Non-Proprietary Security Policy*. San Antonio, TX: AT&T Services, 2014. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2112.pdf.

Defense Information Systems Agency. *Application Security and Development, Security Technical Implementation Guide (STIG) Version 3 Release 9*. Ft. Meade, MD: Defense Information Systems Agency, 2014.

———. "The UC Approved Products List: Multifunction Mobile Device." September 23, 2014. https://aplits.disa.mil/processAPList.action.

Defense Manpower Research. "Demographics of Active Duty U.S. Military." Statistic Brain, November 23, 2013. http://www.statisticbrain.com/demographics-of-active-duty-u-s-military/.

Department of Defense. *Computer Network Defense (CND)* (Department of Defense Instruction (DODI) O-8530.2). Washington, DC: Department of Defense, March 9, 2001.

———. *DOD Commercial Mobile Device Implementation Plan*, Department of Defense Memorandum. Washington, DC: Department of Defense, 2013. http://www.defense.gov/news/dodcMdimplementationplan.pdf.

———. *DOD Mobile Device Strategy*. Department of Defense Memorandum. Washington, DC: Department of Defense, 2012. http://www.defense.gov/news/dodmobilitystrategy.pdf.

———. *Information Assurance (IA)* (Department of Defense Directive (DODD) 8500.01E). Washington, DC: Department of Defense, 2007. http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf.

———. *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)* (Department of Defense Directive (DODD) 8100.02). Washington, DC: Department of Defense, 2007. http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf.

Director, Command, Control, Communications, and Computers Department (C4). *Marine Corps Commercial Mobile Device Strategy*. Washington, DC: Headquarters, U.S. Marine Corps, 2013. http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/20130411_Marine_Corps_Commercial_mobile_device_strategy_Final.pdf.

Donahue, Brian. "Mobile Malware Captures Keystrokes, Screengrabs." *Threatpost*, January 30, 2014. http://threatpost.com/mobile-malware-captures-keystrokes-screengrabs/103973.

Duggan, Maeve, and Aaron Smith. “Cell Internet Use 2013.” *Pew Research Internet Project*, September 16, 2013. http://www.pewinternet.org/2013/09/16/main-findings-2/.

Education Portal. “What Is a Policy Statement?.” Accessed July 14, 2014. http://education-http://education-portal.com/academy/lesson/what-is-a-policy-statement-definition-examples-quiz.html.

Galloway, Brendan, and Gerhard P. Hancke. “Introduction to Industrial Control Networks.” *IEEE Communications Survey & Tutorials*, 15, no. 2 (Second Quarter 2013): 860–880. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6248648&isnumber=6512259.

Gens, Frank, Danielle Levitas, and Rebecca Segal. “2011 Consumerization of IT Study: Closing the “Consumerization Gap.” July 2011. Quoted in Garry G. Mathiason, Michael McGuire, Gavin Appleby, Philip Berkowitz, Tanja Darrow, Helena Eldemir, Philip Gordon, Jacqueline Gruber, Ben Huggett, Stacey James, Sara Kalis, Henry Lederman, Chris Leh, Johan Lubbe, Cecil Lynn III, Suellen Oswald, Todd Ratshin, George Reardon, Mark Schneider, Paul Weiner, William Weissman, Dylan Wiseman, and Jennifer Youpa. *The “Bring Your Own Device” to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*. The Littler Report. New York, NY: Littler Mendelson, P.C., 2012.

Gordon, Whitson. “Everything You Need to Know About Rooting Your Android Phone.” *Lifehacker*, September 4, 2013. http://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone.

Grim, Nicole. “Marine Corps Mobile Device Strategy Looks to Cut Costs.” *Defense Systems*, July 26, 2013. http://defensesystems.com/Articles/2013/07/26/Marine-Corps-mobile-device-strategy.aspx?Page=1.

Halevy, Ronen. “BlackBerry Secure Workspace for iOS & Android Gets FIPS 120-2 Certification.” *BerryReview*, March 26, 2014. http://www.berryreview.com/2014/03/26/blackberry-secure-workspace-for-ios-android-gets-fips-120-2-certification/.

Hammond, Teena. “Unavoidable: 62 Percent of Companies to Allow BYOD by Year’s End.” *ZDNet*, February 4, 2013. http://www.zdnet.com/article/unavoidable-62-percent-of-companies-to-allow-byod-by-years-end/.

Information Technology Laboratory National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. (FIPS Publication 199). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Inspector General United States Department of Defense. *Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices*. (Report No. DODIG-2013-060). Washington, DC: Department of Defense Office of Inspector General, 2013. http://www.dodig.mil/pubs/documents/DODIG-2013-060.pdf.

Johson, Nicole Blake. "Marine Corps Strategy Could Enable BYOD." *Federal Times*, March 7, 2014. http://www.federaltimes.com/article/20140307/MOB/303070009/Marine-Corps-strategy-could-enable-BYOD.

Joint Task Force Transformation Initiative, and National Institute of Standards and Technology (U.S.). *Security and Privacy Controls for Federal Information Systems and Organizations*. (NIST Special Publication (SP) 800-53 Revision 4). Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Kaneshige, Tom. "How BYOD Puts Everyone at Legal Risk." *CIO*, November 21, 2013. http://www.cio.com/article/2380725/byod/how-byod-puts-everyone-at-legal-risk.html.

———. "Is a Remote-Wipe Policy a Crude Approach to BYOD Security?" *CIO*, September 16, 2014. http://www.cio.com/article/2683902/byod/is-a-remote-wipe-policy-a-crude-approach-to-byod-security.html.

Kash, Wyatt. "Marines Break from Ranks with BYOD Test." *InformationWeek*, April 25, 2014. http://www.informationweek.com/government/mobile-and-wireless/marines-break-from-ranks-with-byod-test/d/d-id/1234840.

Keiser, Matthew D., Kristen E. Ittig, and Emma Broomfield. "Guidance for Federal Government Contractors: What to Do with Your Employees during the Shutdown." *Association of Corporate Counsel*, October 10, 2013. http://www.lexology.com/library/detail.aspx?g=9464bb86-bcca-4e31-a013-ce4ec7448c7e.

Knox, Samsung. "Technical Details." Accessed December 30, 2014. https://www.samsungknox.com/en/products/knox-workspace/technical.

Mathiason, Garry G., Michael McGuire, Gavin Appleby, Philip Berkowitz, Tanja Darrow, Helena Eldemir, Philip Gordon, Jacqueline Gruber, Ben Huggett, Stacey James, Sara Kalis, Henry Lederman, Chris Leh, Johan Lubbe, Cecil Lynn III, Suellen Oswald, Todd Ratshin, George Reardon, Mark Schneider, Paul Weiner, William Weissman, Dylan Wiseman, and Jennifer Youpa. *The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*. The Littler Report. New York, NY: Littler Mendelson, P.C., 2012.

National Institute of Standards and Technology (NIST). *Security Requirements for Cryptographic Modules*. (Federal Information Processing Standards (FIPS) Publication 140-2). Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

National Security Agency Information Assurance Solutions Technical Directors. *Information Assurance Technical Framework (IATF) Release 3.1*. Fort Meade, MD: IATF Manager, National Security Agency, 2002. http://www.dtic.mil/docs/citations/ADA606355.

Novell. "Native GroupWise Encryption. GroupWise 6.5 Administration Guide." Accessed December 18, 2014. http://www.novell.com/documentation/gw65/?page=/documentation/gw65/gw65_admin/data/ak9e3ev.htm.

Olzak, Tom. "Security Basics—Components of Security Policies." *brighthub.com*, May 7, 2010. http://www.brighthub.com/computing/smb-security/articles/2259.aspx.

Pew Research. "Cell Phone and Smartphone Ownership Demographics." Accessed December 22, 2014. http://www.pewinternet.org/data-trend/mobile/cell-phone-and-smartphone-ownership-demographics/.

Samsung. "Verizon Wireless Cell Phones: What Is SE Android??" Accessed December 28, 2014. http://www.samsung.com/us/support/faq/FAQ00057510/75485/SCH-I545ZWAVZW.

Scanlon, Jess. "What Is the U.S.'s Most Popular Smartphone?." *Wall Street Tech Cheat Sheet*, June 4, 2014. http://wallstcheatsheet.com/technology/what-is-the-u-s-s-most-popular-smartphone.html/?a=viewall.

Sheldon, Robert. "How iOS Encryption and Data Protection Work." *Techtarget.com*, February 2013. http://searchconsumerization.techtarget.com/tip/How-iOS-encryption-and-Data-Protection-work.

Souppaya, Murugiah, Karen Scarfone and National Institute of Standards and Technology (U.S.). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. (NIST Special Publication (SP) 800-124 Revision 1). Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Symantec Corporation. "Legal Hold." Accessed January 21, 2015. http://www.symantec.com/page.jsp?id=eic-legal-hold.

Timberg, Craig. “Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police.” *The Washington Post*, September 18, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

Trusted Computing Group. “Trusted Platform Module (TPM) Summary.” Accessed December 29, 2014. http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.

U.S. Equal Employment Opportunity Commission. *Bring Your Own Device—Policy and Rules of Behavior*. U.S. Equal Employment Opportunity Commission (EEOC) fv1c. Washington, DC: U.S. Equal Employment Opportunity Commission, 2012.

U.S. General Services Administration. U.S. Office of Personnel Management. “Standard Form 50, Revision 7/91, FPM Supp. 296-33, Subch. 4.” July 1991. http://www.gsa.gov/portal/forms/download/115474.

U.S. Government Accountability Office. “Antideficiency Act Background.” Accessed October 12, 2013. http://www.gao.gov/legal/lawresources/antideficiencybackground.html.

———. *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*. (GAO-12-757). Washington, DC: U.S. Government Accountability Office, 2012. http://www.gao.gov/assets/650/648519.pdf.

U.S. Office of Personnel Management. “Guidance for Shutdown Furloughs.” October 11, 2013. http://www.opm.gov/policy-data-oversight/pay-leave/furlough-guidance/guidance-for-shutdown-furloughs.pdf.

———. “Pay & Leave Pay Administration Fact Sheet: Overtime Pay, Title 5.” Accessed September 14, 2014. http://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/overtime-pay-title-5/.

United States Attorneys’ Office. *United States Attorneys’ Office Policies and Procedures: Bring Your Own Device (BYOD) Program*. Telecommunications & Technology Development (TTD) Staff Office of the Chief Information Officer (OCIO). (no. 3-16-200-017). Washington, DC: Department of Justice, 2014.

Vinton, Kate. “Mobile Malware Is on the Rise, McAfee Report Reveals.” *Forbes*, June 24, 2014. http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/.

Webster, Tom. “2014 Smartphone Ownership Demographics.” *Edison Research*, April 25, 2014. http://www.edisonresearch.com/2014-smartphone-ownership-demographics/.

White House, The. “Bring Your Own Device, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs.” August 23, 2012. http://www.whitehouse.gov/digitalgov/bring-your-own-device.

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California